Accountability model

and its place in the EU regulation proposal

CAPPRIS Meeting - Rennes March 21st, 2013

Daniel Pradelles - EMEA Privacy Officer

Global Context Dynamics……

Today & tomorrow challenges (Business)

Technical context

- Complex, Global & Multi Dimensional context
- Data flows more Global, Dynamic & Fragmented..
- Exponential increase of data creation / collection

Business context

- Highly dynamic Multi stakeholders game
- Highly rewarding and potentially risky trends
- Data Processing drives Innovation, Business Intelligence & Economic growth
- Some Business **models haven't been "privacy" tested**

We are at a break point… …And this change will NOT slow down

Today & tomorrow challenges (Legal)

Regulatory context

- Uncertainty in all regions and in all Business sectors…
- Globalization and technologies straining the traditional frameworks
- Laws are critical but often lagging behind new technologies
- Too much emphasis on Geography specific criteria
- Limitation on scope of legal compliance tool
- Agreement on fundamental principles but different implementations

…Lack of interoperability between Regional legal Approaches…

Today & Tomorrow Challenges (Societal)

- Social norms may be changing but **protection has to stay**
- New Innovative Business models **not obvious or understandable** by Data Subjects
- Cloud will make it even more “**foggy**”
- Traditional **“Consent & Control” approach** may be not sufficient
- Fear & Doubts are shaping **perception**,
- **Trust** becomes a key requirement
- Data Subjects & Politics concerns drive **increased protections**
- Excessive Reactivity under scandals pressure drives **“impulsive” laws**

- Awkward user experience and potential decreased benefits
- Risk of **slowing down acceptance or killing** new technologies & practice

…. Information Society as a whole pushing for “A” change

The Accountability Project

Accountability Project (1)

5 Fundamental elements… (CIPL Galway project)

Organization commitment to accountability and Internal policies consistent with external criteria. 1

Mechanisms to put privacy policies into effect and including tools, training and education 2

Systems for internal, ongoing oversight and assurance reviews and external verification. 3

Transparency and mechanisms for individual participation 4

Means for remediation and external enforcement 5

Accountability Project (2)

How to measure it? (CIPL Paris project)

1. ***Policies:*** *Existence of binding and enforceable written data privacy policies and procedures that reflect applicable laws, regulations and industry standards.*
2. ***Executive Oversight:*** *Internal executive oversight and responsibility for data privacy and protection.*
3. ***Staffing and Delegation:*** *Allocation of resources to ensure that the organization's privacy program is appropriately staffed by adequately trained personnel.*
4. ***Education and awareness:*** *Existence of up-to-date education and awareness programs to keep employees and on-site contractors aware of data protection obligations.*
5. ***Ongoing risk assessment and mitigation:*** *Implementation of a process to assist the organization in understanding the risks to privacy raised by new products, services, technologies and business models, and to mitigate those risks.*
6. ***Program risk assessment and validation:*** *Periodic review of the totality of the accountability program to determine whether modification is necessary.*
7. ***Event management and complaint handling:*** *Procedures for responding to inquiries, complaints and data protection breaches.*
8. ***Internal enforcement:*** *Internal enforcement of the organization's policies and discipline for non-compliance.*
9. ***Redress:*** *The method by which an organization provides remedies for those whose privacy has been put at risk.*

Accountability Project (3)

Incentives and How making it Scalable? (CIPL Madrid project)

> ***"While the principles of accountability would apply to all organizations, their implementation would be custom-designed……All programs, however, will share several common characteristics"***

- Benefits:
  - Heighten the confidence of individuals and organizations
  - Lead to higher levels of compliance
  - Enhance data protection efficiency
  - improve the quality of data protection
  - Better position regulators to police marketplace;
  - Create an expectation in the marketplace
  - Bridge data protection regimes across jurisdictions,

- Two levels of Accountability
  - *General accountability*
  - *Recognized Accountability*

Accountability definition

“Accountability is the obligation to act as a responsible steward of the personal information of others, to take responsibility for the protection and appropriate use of that information beyond mere legal requirements, and to be accountable for any misuse of that information.”

The Galway Project working definitions

.. ***And to be implemented efficiently ..***

..it has to be a Company Culture and a Mindset

A third way between Regulation & Self regulation

HP Data Protection Strategy

Privacy Risk Model
for an Accountable company

1. Compliance Risk
2. Reputation Risk
3. Investment Risk
4. Reticence Risk
5. Business Continuity Risk
6. Compounding Risk

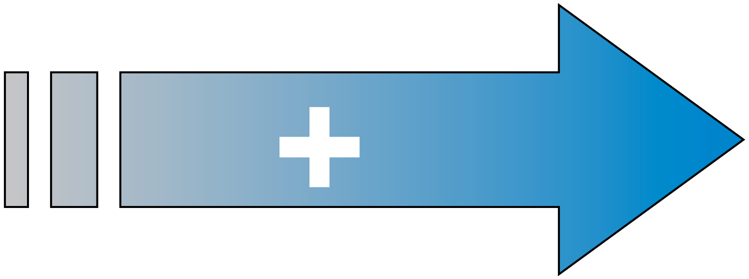
+ Data Subject Risks

& Expectations

Accountability:

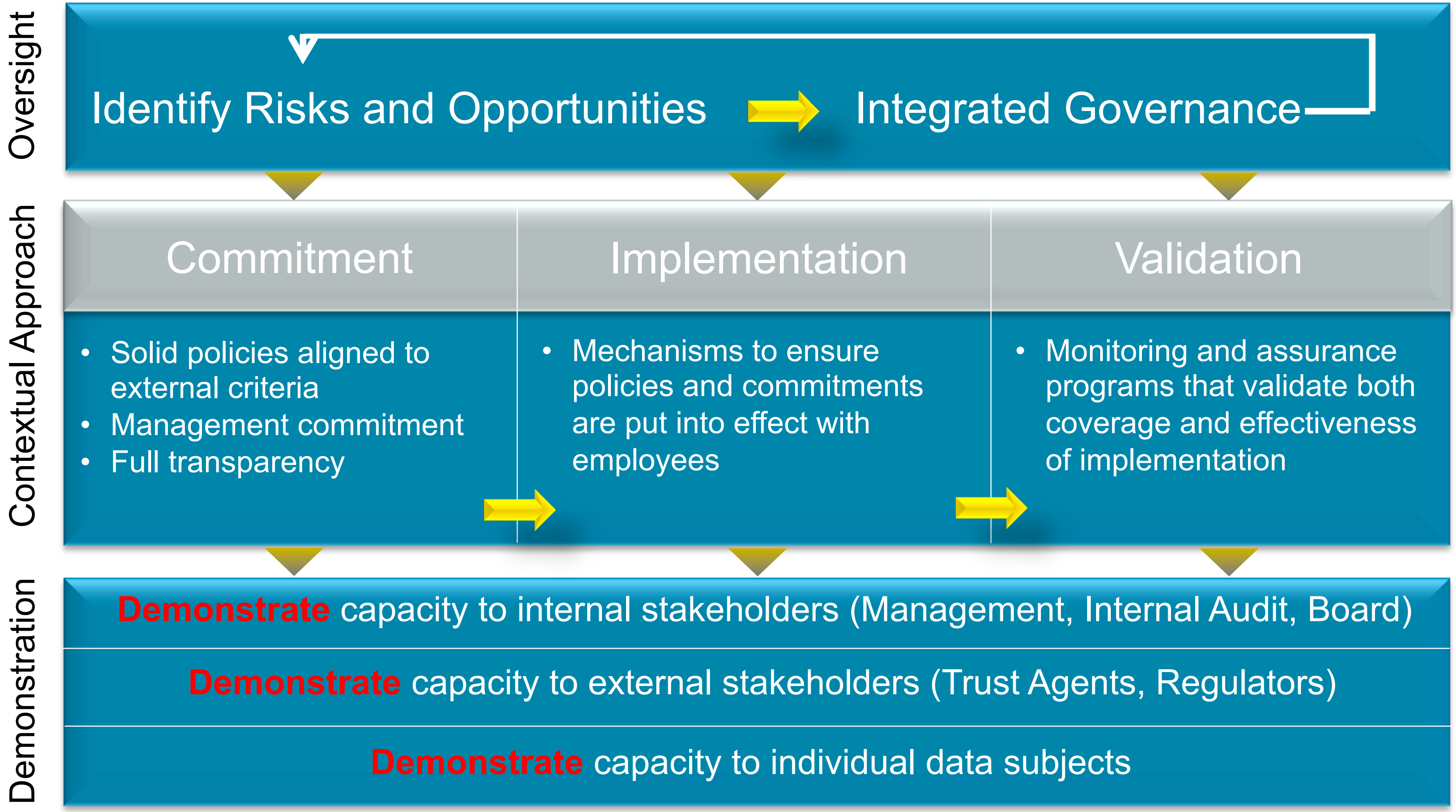
Moving to Accountability culture

Liability	Accountability
Decisions are made based on local laws and regulations ➢ Based on theoretical compliance ➢ Focuses on the minimum standard ➢ Target on known technologies & practices	**Decisions are made based on a set of ethics- and value-based criteria in addition to liability** ➢ All employees accountable for stewardship of data under their charge ➢ Effective privacy handling ➢ Based on expectations and reputation risks



Privacy Accountability Framework

Processes AND Demonstration of Capacity



Oversight

Identify Risks and Opportunities → Integrated Governance

Contextual Approach

Commitment

- Solid policies aligned to external criteria
- Management commitment
- Full transparency

Implementation

- Mechanisms to ensure policies and commitments are put into effect with employees

Validation

- Monitoring and assurance programs that validate both coverage and effectiveness of implementation

Demonstration

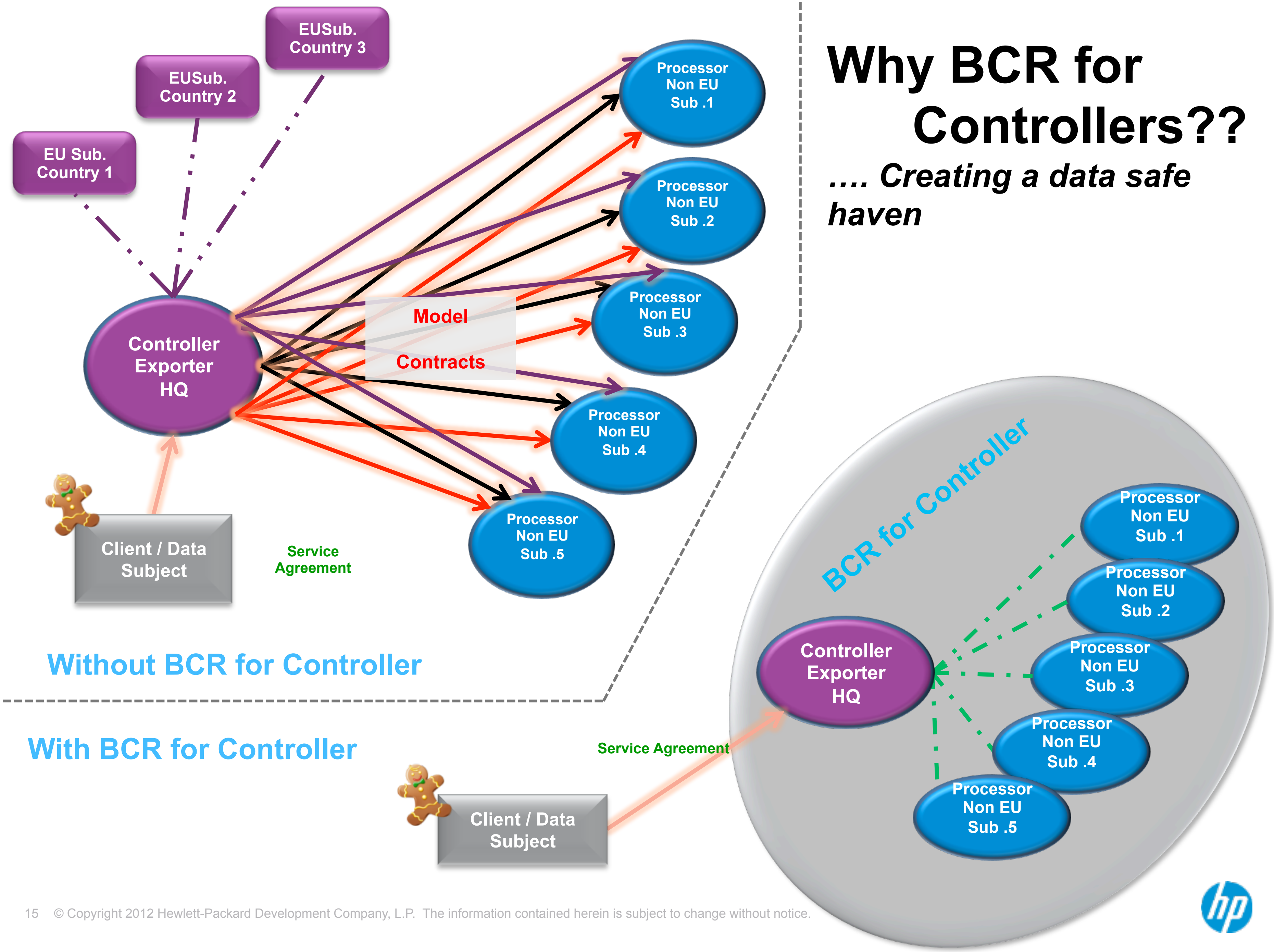
Demonstrate capacity to internal stakeholders (Management, Internal Audit, Board)

Demonstrate capacity to external stakeholders (Trust Agents, Regulators)

Demonstrate capacity to individual data subjects

Why BCR for Controllers??

…. Creating a data safe haven



BCR for Controller ?

It provides:

- EU directive **compliance** for WW Intra Company transfers
- **Flexibility** adapted to Global Business models technologies.
- **More than just Compliance** for transfers

It is a Framework:

- **Demonstrating** Company Capacity to ensure Accountability
- Ensuring **effective** Privacy / Personal Data Protection,
- Fostering **Trust** from Customers, 3rd Parties, Employees & Regulators.

It is a Package:

- EU approved summary (WP133)
- Binding mechanism via Intercompany agreement
- DPA approved compliance with EU requirements (WP153)
- Detailed description of HP Policies, Guidelines and processes, Audit, Training, Privacy Organization,… (WP154)

- HP’s position on EU Regulation proposal

EU Proposal: Data Protection Regulation + Directive

At a glance…

25th January 2012 EU Commission published:

- Draft General Data Protection Regulation
- Draft Directive on processing for Law enforcement activities

Aims

- Accommodate rapid technological change
- Harmonisation
- Reduction of administrative burden
- Putting individuals in control
- Fit with Digital single market
- Address Data Protection in a Globalized World

Regulation will have direct effect

- Delegated Acts of Commission
- Member States - Restrictions and Limited local variations

EU Data Protection Regulation

Main Key messages & New Key concepts

Key messages:

- Individuals' right to enjoy **effective control** over their personal information,
- **Enhance trust** in online services to fulfill the potential of the digital economy,
- Stimulate **economic growth**, create new jobs and foster innovations.

New Key concepts

- **Right to be forgotten**
- Responsibility # Accountability
- Data Portability
- **Privacy by Design**
- Privacy by Default
- **Data Protection Impact Assessments** (risky processing)

EU Data Protection Regulation

Strengthening existing ones and simplifying… a few

Strengthening existing concepts

- Reinforced right to Information (in particular children)
- **Free, Explicit Consent** based on clear Affirmative action (Opt In)
- Improved exercise of Data Subject rights
- Processing description
- DPA independence and powers
- **Increased administrative** and judicial remedies
- Data **breach notifications** generalized
- Privacy enhancing technologies & **Privacy certification** scheme
- **Data Protection Officer mandatory** (for company > 250 employees)

Simplifying…

- Notifications but……
- One stop shopping with applicable law (not obvious) but….
- Improve cooperation between DPA's but….
- WP29 replaced by European Data Protection Board but …..

HP Core principles for the Regulation tuning

- Privacy is a **fundamental right**
- **Supports regulation**
- Companies should be **Accountable**
- EU **Harmonization** is a must
- Global Regulatory **Interoperability**
- Complex Global system requires **fluid & flexible tools**

HP Provided detailed list of suggested amendments

& implementing key stakeholders outrea

HP – Red Flags

- Administrative burden somewhat addressed
- Accountability Concept not fully applied
- Still too rigid & prescriptive
- DPO role incomplete
- BCR including BCR for Processor to develop
- Fines and more??
- Security breach notification
- Responsibilities and liabilities of data processors
- Consent – mechanisms

HP – position on current “Albrecht report”

☺ Customer friendly Approach

☺ EDPB role & Delegated acts

☺ Pseudonimization

☺ Addressing Profiling

☺ Traces of Accountability

☹ Missing Accountability definition

☹ Privacy Officer role

☹ Data Breach threshold and timing

☹ Still very prescriptive

Vision of Accountability in the future…

Cloud privacy questions

Do we have all answers?

Is data safe all across the cloud?

Is it handled based on users expectations?

Is data handling compliant with laws and regulations?

Is data under control along its full lifecycle?

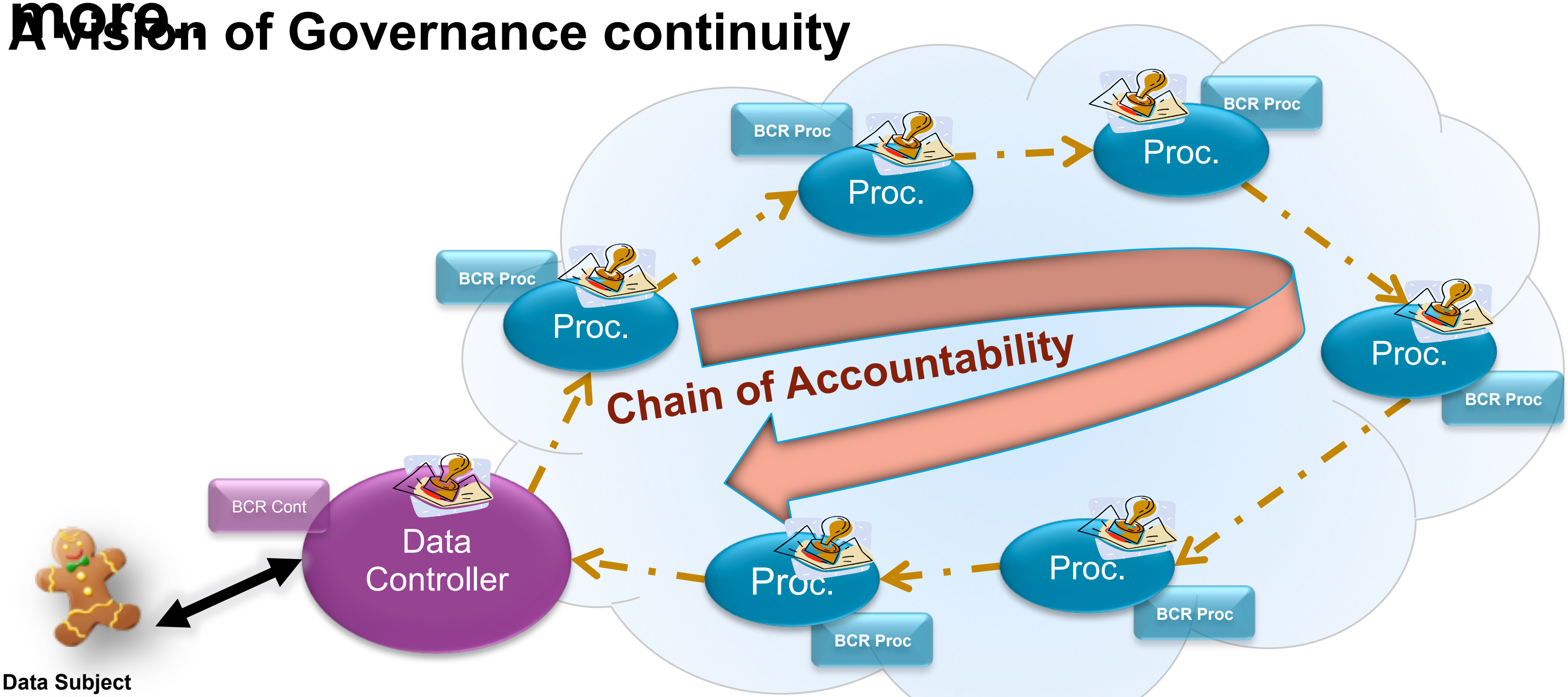
Is appropriate data use & obligations ensured along the Processing chain?

Are there standards or general practices in place for operating in the Cloud?

Organizations ’ legal & moral’ obligation of ensuring privacy and thereby demonstrating the trustworthy nature of their service.

How to achieve effective Privacy in Cloud & more..

A vision of Governance continuity



Open Questions:

- Controller Vs BCR Processor liability linkage?
- Intra Corp. BCR Controller Vs BCR Processor linkage?
- Inter Corp. BCR Controller Vs BCR Processor linkage?
- Inter Corp. BCR Controller Vs BCR Controller linkage?

Accountability Demonstration ?

Privacy today and beyond (Cloud, Internet of things, Big data, etc…)

It should be addressed by:

Consistent and Coordinated development

- in 3 main Dimensions

- with Active collaboration between ALL stakeholders:

- **Responsible Company Governance** (Accountability)
- **Supporting Technologies** (Access Governance, Obfuscation, Data Minimization….)
- **Innovative Regulatory Frameworks** (International Standards and Tools i.e. BCR, CBPR…)

A4 CLOUD

Thanks for your attention

Daniel Pradelles – EMEA Privacy Officer