



31

Medida 4.5 y 6 de noviembre 2009  
conferencia internacional  
de autoridades de protección  
de datos y privacidad

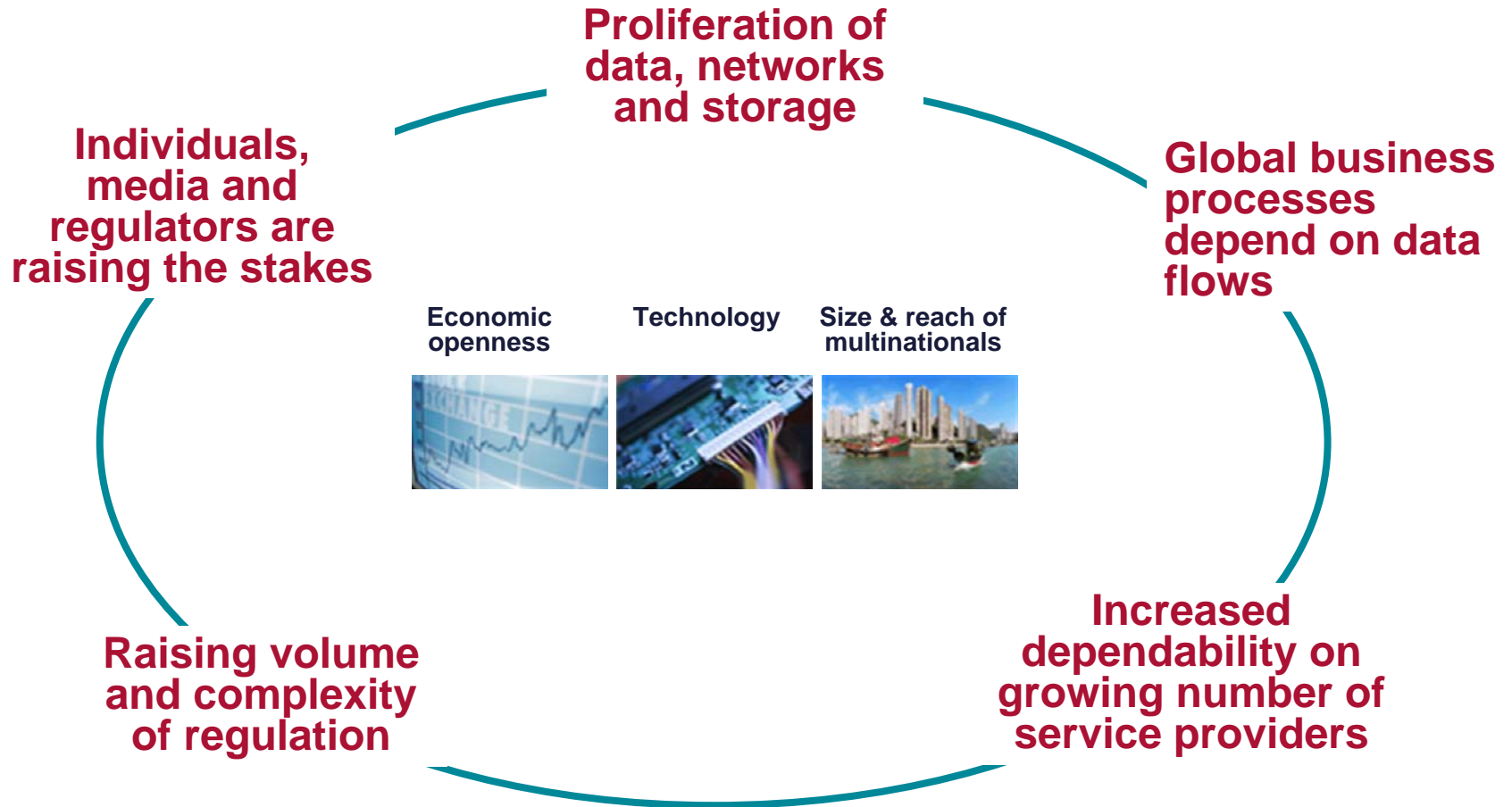
*High performance. Delivered.*

## Data Privacy Corporate Responsibility in Multi Polar World

**Bojana Bellamy**

**Director of Data Privacy, Accenture**

# Why is data privacy different in multi-polar world?



# The law alone is not enough to protect individuals and their data



- Laws suffer from either vagueness or specificity and do not offer global solutions to global problems
  - A requirement for “appropriate” security creates a standard, but no direction
  - Consent per se does not deliver compliance, but may burden individuals
  - Encryption is a defence today, but not tomorrow
- Global companies have to translate requirements into practice and deliver compliance



# Reliance on contracts alone is inadequate in multi-polar world



- Bi-lateral contracts are unrealistic with multiple “controllers” and “processors” in data processing chain, often in multiple locations
- In reality data controllers take one of two approaches, and neither works well:
  - “Hands-off”—try to force the service provider to figure out the controller’s legal compliance responsibilities, or
  - “Hands-on”—try to micromanage the service provider with huge volumes of specific written policies and procedures
- Service providers are left to rationalize each client’s particular requirements while trying to offer standardized services
  - Overlapping multiple contractual requirements create economic inefficiencies and may be hard to implement in practice
- Service providers increasingly have direct legal requirements (HIPAA, Massachusetts)

# The Accenture approach



- Corporate data privacy and protection programs, applicable to and mandatory for all employees and all Accenture companies worldwide
- Part of Code of Business Ethics

## Accenture Data – Binding Corporate Rules

## Client Data – Client Data Protection Program

- Establish a uniform high level of data protection for all personal data, regardless of origin and location, but leave space for customization based on local law or a particular client requirements



## Objectives of Accenture's DP programs

- Minimize regulatory, contractual and financial risks
- Avoid reputation and brand erosion
- Build trust of clients and our people
- Position the company as an industry leader



# Ensuring and measuring compliance - seven standards approach



Policies and  
procedures

Oversight  
function

Delegation  
of authority

Education  
and  
awareness

Enforcement  
and  
discipline

**Effective Compliance**

Monitoring  
and  
auditing

Response  
and  
prevention

# Some key communications



**Data protection  
Dos and Don'ts**

Learn your key actions to protect client information.

**Client Information  
Your Responsibility**

accenture  
High performance. Delivered.

• Consulting • Technology • Outsourcing

Data Privacy posters distributed globally

**Protect Personal Privacy**

accenture  
High performance. Delivered. Comply with Data Privacy Policy 90

• Consulting • Technology • Outsourcing

Dos and Don'ts tailored by level and Growth Platform

**Client Data Protection**

The Accenture Client Data Protection program

Accenture's Client Data Protection program consists of the following components:

1. Client Data Protection Program Management - general management, administration and continuous improvement of Client Data Protection Program
2. Client Data Protection Program - specific management, administration and continuous improvement of Client Data Protection Program
3. Client Data Protection Program - specific management, administration and continuous improvement of Client Data Protection Program
4. Client Data Protection Program - specific management, administration and continuous improvement of Client Data Protection Program

Client Data Protection Site

**Bojana Bellamy on the impact of data privacy and data protection to Accenture, clients and you**

Bojana Bellamy, Accenture Chief Data Privacy Compliance Lead

As part of our Data Privacy and Compliance program, we are pleased to share the results of our work with you.

As a result, what are data privacy laws?

Accenture is committed to protecting your information and ensuring that your data is secure and private. We are committed to ensuring that your data is secure and private.

Dialogue Online article and discussion board

# Data Privacy Day 2009



Global Data Privacy > Data Privacy Day 2009

## Accenture Celebrates Data Privacy Day 2009

Know How to Protect your personal data



Protecting Accenture Personal Data

Data Privacy Day 2009



Protecting Your Personal Data



Protecting Client Personal Data

Global Data Privacy  
High performance. Delivered.

### Ten Ways Accenture Protects Your Personal Data

Safeguarding our people's personal data is one of Accenture's most important responsibilities. What is personal data? It is any data that relates to a living person who can be identified from the data set. This includes, among other things, your name, email and postal address, social security number or other national ID numbers, photos, audio recordings and performance evaluation.

Most countries in which Accenture operates have specific laws that regulate how we collect, use, store, access, and share our people's personal data. These laws are not just about the duties of the company, but also the rights individuals have with respect to information held about them.

Accenture works to make certain your personal data is used appropriately in accordance with data privacy laws. The following are some of the steps we take to comply with data privacy laws and protect your personal data.

1. Our data privacy compliance program is leading-edge

Our global data privacy compliance program has earned us praise and recognition from clients, peers and data privacy regulators around the world. In Europe regulators have granted preliminary so-called "Binding Corporate Rules" approvals based on our program which will allow us to transfer your personal data around the world within our global organization without the need for additional permits or formalities. Whilst we must still complete the formal procedures, this shows that the regulators are satisfied that the safeguards in our program are strong enough to protect your data. Our program's objectives are to make sure that local Accenture companies comply with local data privacy laws; mitigate the risk and impact of these laws on our operations and internal functions; allow us to share data across our global organization; and enable us to become industry leaders in this field. Our global data privacy compliance program was established in 2000 in response to Accenture's rapid growth and the need to comply with increasingly complex data privacy laws globally. We review our data privacy compliance program on a regular basis to make certain it is up to date and complies with laws and regulations around the world.

Global Data Privacy  
High performance. Delivered.

### Know How to Protect Your Personal Data

Imagine this scene. You get home from work and there is a letter from your bank explaining that one of its employees has had an unrecalled laptop stolen. Unfortunately the employee had downloaded tens of thousands of account holder details to use in a test database.

The bank cannot guarantee that your personal data has not been compromised, nor that it is not in the hands of criminals who could use it to steal your identity or commit fraud. You check your online bank account and are horrified to see that several large payments have been withdrawn without your due. The bank agrees to investigate whether this is linked to the loss of your personal data but you still have to prove you didn't authorize the money.

Your personal data is valuable, so you should treat it as you would any other valuable item. With comes the identity that on the rise, it is even more important to safeguard your personal data.

1. What is personal data?
2. Why is managing your personal data important?

Here are a few practical steps you can take to protect your personal data and that of others from misuse:

1. Learn about your data privacy rights

Many countries have data privacy laws. Find out if your country has privacy laws by contacting your local Data Protection Office, your country's data protection authority, or your local consumer protection agency.

Global Data Privacy  
High performance. Delivered.

### Data Security: Your Responsibility to Protect Your Client's Data

Did you know that loss or theft of laptops and mobile devices with confidential data has resulted in huge fines, loss of clients and a tarnished reputation for many companies? Privacy regulators are ordering companies to encrypt portable media devices and businesses are facing regulatory and commercial repercussions in the form of fines and loss of contacts.

Accenture's business is based on our reputation and the trusted relationships we have with our clients. Therefore, it is critical that we protect the data entrusted to us by our clients – this includes personal data, business data and intellectual property. In an effort to maintain the security of our client's data, Accenture relies on [Data Encryption Software](#) (see [Data Encryption Software](#)) when a computer's hard drive is encrypted, the data can not be easily accessed in the event the computer is lost or stolen.

In addition, all standard workstations provided by Accenture include [Trend Micro software](#), [Avast software](#) and [Data Encryption Software](#). Accenture also has a team that monitors security software vulnerabilities uncovered in the market and silently distributes security patches for these vulnerabilities as needed.

Unfortunately, technology alone can not prevent information from being compromised. Therefore, Accenture places an emphasis on the education of our people regarding security risks, the requirements of our security policies and the steps we can take to ensure the data entrusted to us remains secure.

In January 2008, all employees will be required to take data privacy and information security training. This training will clarify our employee's responsibilities regarding the protection of client data and the steps they can take to protect the data entrusted to them.

It is critical you take all mandatory training including [Data Privacy - What It Means and Why It Matters](#) currently available on [mLearning](#). In addition, you should follow Accenture's security policies and practice good security behaviors such as:

- Encrypting all data stored on mobile devices (e.g. USB drives)
- Removing data from all storage devices when no longer needed
- Storing project deliverables on a team share point site, not just your own computer

Data Security – Your responsibility to protect client data

## Ten Ways Accenture Protects Employee Data

# What lies ahead?



- A legal model where each party processing personal data implements comparable set of requirements and is accountable for its own conduct and protection of data
- A decreased emphasis on contracts as the primary tool for protecting data
- Greater endorsement by DP regulators of effective and verifiable seven-standards based data privacy systems — BCR for controllers and BCR for processors; accountability model.