NAIR&CO.

Keeping Private Data Private

NAIR&CO.

The Challenges

- Regulations – Privacy Rules
- Regulations – Money Laundering
- Cloud Computing
- Reporting Standards Of Service Providers
- Social Networking Sites
- Employee Blogs

NAIR&CO.

Existing Regulations - EU

- Somewhat harmonious regulations
- Governing Directive is reg 95/46/EC
- Each country has enacted differently
- All countries require consent before processing personal data
- Many require registration with central authority

Existing Regulations – Other Countries

Latin America – Argentina, Brazil, Chile, Columbia, Mexico, Peru

East Europe – Bulgaria, Czech Rep, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slovak Rep, Slovenia.

Asia – Hong Kong, India, Japan, Korea, Singapore, Taiwan, Thailand, Vietnam.

NAIR & CO.

New Regulations

- China – New Draft Privacy Rules Jan 2011
- India – New Rules April 2011
- Canada – New Anti-spam Laws From Fall 2011
- EU – Updating 1995 Directive

Keep Abreast of Changes in Law
Check For Changing Rules in Countries Where You Operate
Check Your Processes – Do They Comply?

NAIR&CO.

Money Laundering Regulations

Privacy Rules = No Disclosure Without Consent

But

Money Laundering Rules = Reporting With***out*** Informing Customer

Do Your Client Agreements Protect You?

(Ts & Cs Of A Major Credit Card Company Does Not Protect Them!)

NAIR&CO.

Cloud Computing

Cloud Services in Different Locations = Personal Data Across Jurisdictions
but
Responsibility To Protect Data Remains **Yours**

Check geographic location, data retention and security of provider
and
How you will monitor that cloud provider/user adheres to your terms especially protection of data?

Service Providers' Reporting Standards

- Service providers are among your highest risks
- AICPA new guidance (SOC 2, Reports on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy) being developed
- Will be type 1 and type 2 reports as for SOC1

In Absence of SOC2, Discuss Controls and Agree Reporting Mechanism

NAIR&CO.

Social Networking (SN)

- Companies promote on SN sites
- Data on site is outside control of the company
- How do employees know what information to use?

Review policies on what data should be on site and communicate policies clearly to employees

Does Your Staff handbook covers this?

NAIR & CO.

Employee Blogs

Is a growing problem

Many target specific employers and their practices

Define and prohibit sensitive information

Ban company name from such sites

Warn company will take action against breaches

NAIR & CO.

Penalties

- **Argentina –** Fines Up To $100,000, **Erasure of Data**
- **Denmark** – Fines, Imprisonment, **Suspension of Business**
- **France** – Fines, Imprisonment**, Ceasing Processing Operations**
- **U.K. –** Fines up to **GBP 500,000,** Imprisonment, **Erasure of Data**
- **Canada** – Fines up to **C$10,000,000** on Corporations

Summary of Actions

- Keep Abreast of Rules in Countries You Work
- Check Your Employee Agreements and Vendor Contracts
- Review Policies and Communication
- Check How You Communicate Internally e.g. Pay Reviews
- Review Your Service Providers and Ask for Reports – SOC 1 And SOC 2