# Compliance, the Digital Environment and Data Protection: Why and How Your Business Must Be Prepared

Marcelo Crespo – Lawyer and Professor
Liana Cunha – Compliance Coordinator

## The Digital Environment

- *Cyberspace is like Oz: it is, we get there, but it has no location*

Nicole Stenger
(French born American artist, pioneer in Virtual Reality and Internet movies)

## Digital Environment…

- …is not perfectly synonymous:
  - with digital technology, or
  - with the ubiquity of the internet, or
  - with the move from analogue to digital broadcasting, or
  - with the mass appeal of mobile phones, or
  - with the proliferation of information and the demise of the expert, or
  - with the commercial and political strategies associated with globalization and commercialization, or even
  - with the ubiquity of the personal computer.

## Digital Environment

- The Digital Environment is the conglomeration of all of those events, facts, realities into a tangible experience of a changed way of being.
- Therefore, it is a complex scenario that must be studied and daily understood.

## Data protection: an overview

- We will present an overview of data protection in:
- USA
- Europe
- Brazil

## Data protection in USA

- There is no single comprehensive federal law regulating the collection and use of personal data.
- There is a patchwork system of federal and state laws and regulations that overlap, dovetail and may contradict one another.
- In addition, there are self-regulatory efforts considered “best-practices” made by governmental agencies and industry groups.

# Data protection in USA

- Federal Privacy Laws:
  - Children Online Privacy Protection Act – COPPA (2012/2013)
  - Personal Data Protection and Breach Accountability Act (2014)
  - Data Broker Accountability and Transparency Act (2014)

# Data protection in USA

- Sectoral Laws
  - Federal Trade Commission Actc (15 U.S.C. §§41-48)
    - Federal consumer protection law that prohibits unfair or deceptive practices and has been applied to offline and online privacy and data security policies..
  - The Financial Services Modernization Act (Gramm-Leach-Bliley – GLB – 15 U.S.C. §§6801-6827)
    - Regulates the collection, use and disclosure of financial information.
  - The Health Insurance Portability and Accountability Act (HIPAA – 42 U.S.C. §1301 et seq.)
    - Regulates medical information.

# Data protection in USA

- Sectoral Laws
  - The Fair Credit Reporting Act (15 U.S.C. §1681)
    - Applies to consumer reporting agencies such as lender and credit card companies.
  - The controlling the assault of non-solicited pornography and marketing act (CAN-SPAM Act – 15 U.S.C. §§7701-7713)
    - Regulates the collection and use of email addresses and telephone numbers.

# Data protection in USA

- State Laws:
  - There are many laws at state level that regulate the collection and use of personal data.
  - Most states have enacted some form of privacy legislation, however, California leads having enacted multiple privacy laws (including a Security Breach Notification Law).
  - March 2014: 46 states have enacted laws requiring notification of security breaches involving personal information.

## What acts are regulated?

- Mainly:
  - Fail to protect consumer personal data
  - Privacy policies changes without adequate notice
  - Fail do comply with a posted privacy policy

## What are the main obligations imposed on data controllers?

- Data encryption
- Authentication mechanisms
- Background checks
- Frequent monitoring and testing information security protocols and systems
- Ensure the security and confidentiality of customer records

## What are the main obligations imposed on data controllers?

- Protect against any anticipated threats or hazards to the security or integrity of these records
- Implement an identity theft prevention programme.
- Implement response programme regulations the financial institutions to notify the regulator when there has been unauthorized access to sensitive customer information

## Data protection in Brazil

- As in the USA, there is no single comprehensive federal law regulating the collection and use of personal data.
- There are some federal laws: a) Federal Constitution; b) Legal Framework for consumer protection (nº 8.078/90); Law of the compliant debtors (nº 12.414/11); Law on access to public information (nº 12.527/11); Legal Framework for the Internet ("Marco Civil da Internet") (nº 12.965/14)
- Despite the regulation mentioned above, there are breaches.

## Data protection in Brazil

- Brazil has a Bill Draft being discussed.
- The draft intend to provide a federal and general regulation for personal data.
- It defines data, personal data and creates procedures on personal data collection.
- It indicates the responsibilities of those who collect, use and transfer personal data, including third parties.

## Data protection in Brazil

- Europe does not have a legislative act on Data Protection.
- Although, there is a Directive (nº 95/46/EC) on the protection of individuals with regard to the processing of personal data within the European Union.
- In January 2012 the European Commission unveilled a draft for General Data Protection that, sometime, will supersede Directive nº 95/46/EC.

## Data protection in Europe

- Europe does not have a legislative act regulating personal data.
- Although, there is a Data Protection Directive (nº 95/46/EC) with regard to the processing of personal data.
  - Sets out a goal that all EU countries must achieve. However, it is up to the individual countries to decide how
- On January 2012, European Commission unveiled a draft for a General Regulation that will supersede the Directive above mentioned.
  - It must be applied in its entirety across the EU.

## Data protection in Europe

- It establishes that personal data should not be processed at all, except when certain conditions are met:
  - Transparency;
  - Legitimate purpose;
  - Proportionality.

## Data protection in Europe

- The responsibility for compliance rests on the shoulders of the "controller" (a natural or artificial person, public authority, agency or any other which determines the purposes and means of the processing data.
- Supervisory authority
  - Each country must create an independent body that will monitor the data protection level in that member state, give advice to the government about administrative measures and regulations, and start legal proceedings when data protection regulation has been violated.

## Compliance Role

- Considering the complexity of data privacy regulation, this issues must be seriously observed in compliance programs.
- Compliance works with:
  - Building and protecting Reputation;
  - Analyzing risk;
  - Developing procedures and policies to guarantee the compliance with all regulations about the topic;
  - Providing awareness of the importance of these processes;
  - Training and monitoring activities to prevent any wrong procedure or undesired results;

## Compliance

- Being compliant means following processes and policies to guarantee that all Legal and Regulatory aspects are being dully followed;
- It is necessary to ensure that the organization follows its processes to protect personal data from employees, clients and third parties to which the company deals with.

## Do's and Don'ts

- Map for compliance Success:
  - Work together with all areas of the company to understand what is sensitive data
  - Differ data from sensitive data for each kind of business, considering risk and the diversity of regulation
  - Help to develop, analyze, and implement ways of collecting and disclosing data respecting individual rights
  - Set up strategic meetings with the Board and key leaders of the company to have a conscious governance, taking decisions and implementing tools according to the risk (BYOD, labor, intellectual property and so on)

# Do's and Don'ts

- Map for compliance Success:
  - Implement prevention programs in order to keep personal data secure at all times;
  - Regulate the terms under which intra-group transfers of personal data are made need to be assessed;
  - Be aware and exam transfers of personal data across borders in order not to infringe foreign law;
  - Implement internal procedures to ensure continuing compliance with the above and the effective handling of enquiries and complaints by individuals.

# Do's and Don'ts

- Map for compliance Success:
  - Help implementing clauses at agreements to guarantee its accomplishment and also to contemplate audit clauses – inserting third parties to do that, when appropriate – avoiding any risk to the company;
  - Implement internal tools that allow employees to inform any risk or wrong action that is being taken or can possibility be understood like this;
  - In case of any allegation comes, work with a remediation plan to stablish the secure atmosphere business needs.

# The end!

- Thank you very much for your attention!
- Any doubts? Feedback?
- marcelo@cresposantos.com.br
- liana.cunha@abbott.com