Plenary Session 2:
Data Privacy Law Compliance

Matrix of Legal Requirements

The CHAMBER Connects

Atty. Marcelino Arias, Jr.

Republic Act No. 10172

- Data Privacy Act of 2012 (August 15, 2012)
- An Act Protecting Individual Personal Information and Communication Systems in the Government and Private Sector
  - Protect Fundamental Human Right of Privacy and Communication while ensuring free flow of information
  - Ensure that personal information in Information and Communication Systems (ICS) are secured and protected

What is protected?

- **Personal Information** - any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably or directly ascertained by the entity holding the information or when put together with other information would directly and certainly identify an individual

Who are Covered?

- Those involved in the processing of personal data in the Philippines
- Those involved in processing of personal data of a Philippine Citizen or Resident
- Those entities with links in the Philippines which may include branch offices, agencies, incorporated foreign businesses, that holds personal data in the Philippines

Other Classes of Personal Data

- **Privileged Information**

- **Sensitive Information**
  - Race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliation
  - Health, education, genetic or sexual life of a person
  - Proceedings/Offenses committed and its disposition
  - Government Issued Documents, SSS, licenses, tax returns, etc.
  - Those specifically established by law to be kept classified

Case Study on Personal Information

Facts:

Worten, a private company in Portugal, adopted a system which restricts the access to the working hours of its employees. The system did not permit ACT to have automatic access. ACT considered the failure to have automatic access as a serious offense against Portugal's national law and imposed a fine against Worten.

Issue:

Whether or not the record of working time for each employee is covered by the concept of personal data under Article 2 of Directive 95/46.

Case Study on Personal Information

Ruling:

- Data contained in a record of working time concerning, in relation to each worker, the daily work periods and rest periods, constitute personal data because they represent “information relating to an identified or identifiable natural person”.

What is Data Processing?

- Any operation performed upon personal data:
  - Automated or Manual
  - Physical or Electronic
- Includes collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidated, blocking, erasure or destruction of data.

Data Processing Case Study

- **Facts:**

- Lindqvist was charged with violation of Swedish Data Protection Law for publishing on her internet site personal data on a number of people working with her on a voluntary basis in the Swedish Protestant Church.
- Lindqvist published on the internet the names, jobs, hobbies, telephone numbers, and family circumstances etc. of 18 colleagues, as well as the fact that one had injured her foot and was on medical leave without informing them of the existence of the internet page and without obtaining their consent. She also failed to notify Datainspektionen of her activity. She removed the pages in question as soon as she became aware that they were not appreciated by her colleagues. Lindqvist was later on prosecuted for violation of the Swedish Data Protection law.

Data Processing Case Study

- **Issue:**

Whether the act of referring, on an internet page the name of a person or of personal data (telephone number or information regarding their working conditions and hobbies) constitutes *automatic processing of data* within the meaning of Article 3(1) of Directive 95/46/EC.

Data Processing Case Study

Ruling:

The term personal data used in Article 3(1) of Directive 95/46 covers, according to the definition in Article 2(a) thereof, any information relating to an identified or identifiable natural person. The term undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies.

Data Processing Case Study

Ruling:

According to the definition in Article 2(b) of Directive 95/46, the term processing of such data used in Article 3(1) covers any operation or set of operations which is performed upon personal data, whether or not by automatic means. That provision gives several examples of such operations, including disclosure by transmission, dissemination or otherwise making data available. It follows that the operation of loading personal data on an internet page must be considered to be such processing.

Key Persons in Data Protection

- **Data Subject**
  - Individual whose personal information is processed.
- **Personal Information Controller (PIC)**
  - Controls or Instructs another to process personal data - determines what information is to be collected, its purpose and extent.
- **Personal Information Processor (PIP)**
  - Processing of personal information is delegated by the data controller.

Principles in the Processing of Personal Data

- Processing of Personal Data is allowed subject to the requirements of law
- Personal Data Processing should be:
  - Transparent - informed consent
  - Legitimate purpose
  - Proportionate
  - Accurate (Data Quality)
  - Data Retention and Disposal consistent with legal and industry standards

Principles in the Processing of Personal Data

- Data Sharing
  - Allowed only when it is expressly provided by law.
  - In the Private Sector, allowed only when there is:
    - Consent of the data subject (Identity, Purpose, Extent, Recipient, Appraisal of Rights of data subject, etc.)
    - Data Sharing Agreement

Rights of the Data Subject

- ✓Information
- ✓Access
- ✓Object
- ✓Erasure or Blocking
- ✓Damages
- ✓File a Complaint
- ✓Rectify
- ✓Data Portability

Case Study on Right to Object

Facts:

Mr. Schwarz applied to the Stadt Bochum for a passport, but refused to have his fingerprints taken. After the Stadt Bochum rejected his application, Mr. Schwarz brought an action before the referring court in which he requested that the city be ordered to issue him with a passport without taking his fingerprints.

Case Study on Right to Object

Issues:

Whether or not Mr. Schwarz may be issued a valid passport without his fingerprints.

Case Study on Right to Object

Ruling:

Fingerprints constitute personal data as they objectively contain unique information about individuals which allows those individuals to be identified with precision.

In addition, processing of personal data means any operation performed upon such data by a third party, such as the collecting, recording, storage, consultation or use thereof. This means that national authorities are to take a person's fingerprints and that those fingerprints are to be kept in the storage medium in that person's passport. Such measures must therefore be viewed as a processing of personal data.

While a fingerprint is considered personal data and the taking thereof as processing under the data protection law, the taking and storing of the fingerprint was a valid limitation on the rights provided by the data protection law because this is a necessary means to prevent falsification of passports and illegal entry to the country.

Erasure or Blocking Case Study

- **Facts:**

Mr. Gonzales, a Spanish national, sued Google Spain, Google Inc., La Vanguardia newspaper, alleging that when an internet user entered his name in the google search engine, he would obtain links to two pages of La Vanguardia newspaper on which an announcement with his name appeared for a real estate auction connected with attachment proceedings for the recovery of social security debts.

Erasure or Blocking Case Study

Issue:

Whether DPA Spain may order the search engine operator (Google) to remove Mr. Gonzales' information or links to his personal information.

Erasure or Blocking Case Study

The search engine operator must erase information and the links concerned in the list of results if that information appears, having regard to all circumstances of the case to be **inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue** carried out by the operator of the search engine. Here, having regard to the sensitivity of the data subject's private life of information contained in the announcements and the fact that **the initial publication occurred 16 years earlier the data subject has established that the links should be removed.**

Data Privacy and Security

- Reasonable and Appropriate Security Measures
- Organizational
  - DPOs, Internal Policies, Protocols, Manuals, Documentation, Management and Supervision
- Physical
  - Access, Record Keeping, Physical Office Lay-out, Retention/Destruction
- Technical
  - Automated Systems, Computer Network, Electronic Data Sharing, and Applications

Data Breach

- A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.
- Breach that requires notification - sensitive personal information or information that may be used for identity fraud.
- 72 Hour Rule - Duty to notify the Commission upon knowledge of the breach; containing the nature, extent of data, and measure taken.

Compliance under Republic Act No. 10173

- Appointing or designating a Data Privacy Officer and/or Compliance Officer
  - Person accountable for ensuring compliance with the Data Privacy Act
  - Qualification - knowledge of the processing operations, information systems, data security, and data protection needs of the controller or processor; full-time or organic; ideally regular or permanent position; or with at least 2 year term for contractual

Compliance under Republic Act No. 10173

- Internal Compliance Process
  - Adoption of Privacy Policies, Internal Protocols, and Data Privacy Compliance Manual
  - Preparation of Consent Forms
  - Training of Personnel
  - Integration of Technology to Protect Data Security
- Registration with the NPC

Registration of Data Processing Systems

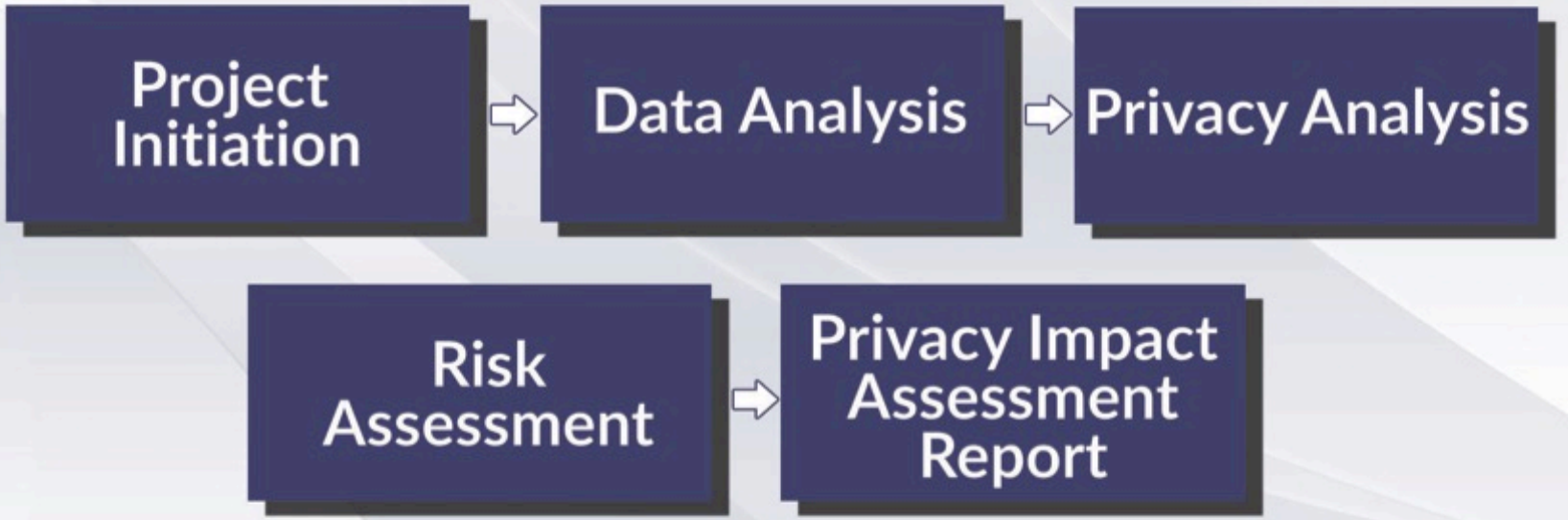
- Data Processing System - refers to a structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing
- Mandatory Compliance
  - A. the PIC or PIP employs at least two hundred fifty (250) employees;
  - B. the processing includes sensitive personal information of at least one thousand (1,000) individuals;
  - C. the processing is likely to pose a risk to the rights and freedoms of data subjects
  - D. the processing is not occasional
- DEADLINE for Registration for data processing systems is MARCH 8, 2018.

Privacy Impact Assessment (PIA)

- A process undertaken and used to evaluate the impact on privacy when personal information is collected and processed.
- Whether the rights of the Data Subject is observed
- Identification of Possible Breaches
- Other requirements of the DPA and/or the NPC

ACHIEVE
WITHOUT BORDERS

Privacy Impact Assessment



Privacy Impact Assessment (PIA)

- Provide a systematic description of the personal data flow and processing activities of the PIC or PIP
- Include an assessment of the adherence by the PIC or PIP to the data privacy principles, implementation of security measures, and provision of mechanisms for the exercise by data subjects of their rights under the DPA
- Identify and evaluate the risks posed by a data processing system to the rights and freedoms of data subjects, and proposes measures that address them
- Ensure the involvement of interested parties and secures inputs from the DPO and data subjects

Why undergo PIA and Compliance

- Because the personal information controller and responsible persons and OFFICERS are held personally liable.
- Including natural or juridical persons or bodies involved in personal data processing.
- Substantial Fines
- Criminal prosecution.

Unauthorized Activities and Penalties

- Unauthorized Processing (Sec. 52)

Persons liable: Those who process personal information without the consent of the data subject, or without being authorized under the law

Penalties:

Personal Information: 1-3 years imprisonment and fine 500k to 2M pesos

Sensitive Information: 3-6 years imprisonment and fine 500k to 4M pesos

- Accessing Due to Negligence (Sec. 53)

Persons liable: Those who, due to negligence, provided access to personal information without being authorized under the law

Penalties:

Personal Information: 1-3 years imprisonment and fine 500k to 2M pesos

Sensitive Information: 3-6 years imprisonment and fine 500k to 4M pesos

Unauthorized Activities and Penalties (continued)

- Improper Disposal (Sec. 54)

Persons liable: Those who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection.

Penalties:

Personal Information: 6 months to 2 years imprisonment and fine 100k to 500k pesos

Sensitive Information: 3-6 years imprisonment and fine 500k to 4M pesos

- Processing for Unauthorized Purposes (Sec. 55)

Persons liable: Persons processing personal information for purposes not authorized by the data subject.

Penalties:

Personal Information: 1 year 6 months to 5 years imprisonment and fine 500k to 1M pesos

Sensitive Information: 2-7 years imprisonment and fine 500k to 2M pesos

Unauthorized Activities and Penalties (continued)

- Unauthorized Access or International Breach

Persons liable: Those who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information is stored

Penalties:

1 to 3 years imprisonment and 500k to 2M fine

- Concealment of Security Breaches Involving Sensitive Personal Information

Persons liable: Those who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20(f), intentionally or by omission conceals the fact of such security breach

Penalties:

1 year and 6 months to 5 years imprisonment and 500k to 1M fine

Unauthorized Activities and Penalties (continued)

- Malicious Disclosure (Sec. 58)

Persons liable: Any PIC or PIP or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her

Penalties:

1 year and 6 months to 5 years imprisonment and 500k to 1M fine

- Unauthorized Disclosure (Sec. 59)

Persons liable: Any PIC or PIP or any of its officials, employees or agents, who discloses to a third party personal information or sensitive personal information without the consent of the data subject

Personal Information: 1-3 years imprisonment and fine 500k to 1M pesos

Sensitive Information: 3-5 years imprisonment and fine 500k to 2M pesos

Unauthorized Activities and Penalties

- Combination or Series of Acts

3-6 years imprisonment and fine 1M to 5M pesos

- Large-Scale Commission (100 persons)

Penalties in the Maximum

Legal Consulting Services

- Data Privacy Governance & Policies

Assist in the appointment of a Data Protection Officer, draft Data Protection Charter & General Policy Statements

- Risk Assessment / Privacy Impact Assessment

Evaluate Records of Processing Activities & Conduct a Privacy Impact Assessment (PIA) study

- Setting your Data Privacy Rules & Regulations

Draft the organization's Privacy Management Program (PMP)

Develop a Privacy Manual and Complaints Mechanism

Legal Consulting Services

- Evaluate the Daily Personal Information Life Cycle Processes of the Company

Draft policies : to notify data subjects and secure consent ; allow data subjects to object to subsequent processing or changes to the information supplied to them and limit data processing according to its declared, specified and legitimate purpose ; other relevant data privacy rules and procedures.

- Training Management and Internal Organization (i.e. Human Resources)

to respond to the daily challenges of data protection compliance

Regular and compulsory staff training on general privacy and data protection in job areas sensitive to personal information handling and the proper Issuance of Security Clearance for those handling personal data both internal & external.

Assist in the outsource of compliance with the DPA

Legal Consulting Services

- DPO Function Consulting

On-call assistance for DPO functions on a retainer basis.

- Establish Third Party Rules & Agreements

Set up adequate data privacy mechanisms (i.e anonymization) & rules for third parties (e.g. outsource suppliers, clients, vendor, processor, affiliates) and draft third party contracts (Data sharing Agreements, Due Diligence, Notifications, Access Policies) to minimize third party risk.

- Preparation & Registration of your company's Personal Data Processing System with the NPC

Assist in the preparation, submission & registration of the company's Personal Data processing system with the NPC.