Privacy: Principles, Problems & Practices

OCAMPO & SURALVO LAW OFFICES

ATTY. JUDE B. OCAMPO

Data Privacy Luncheon

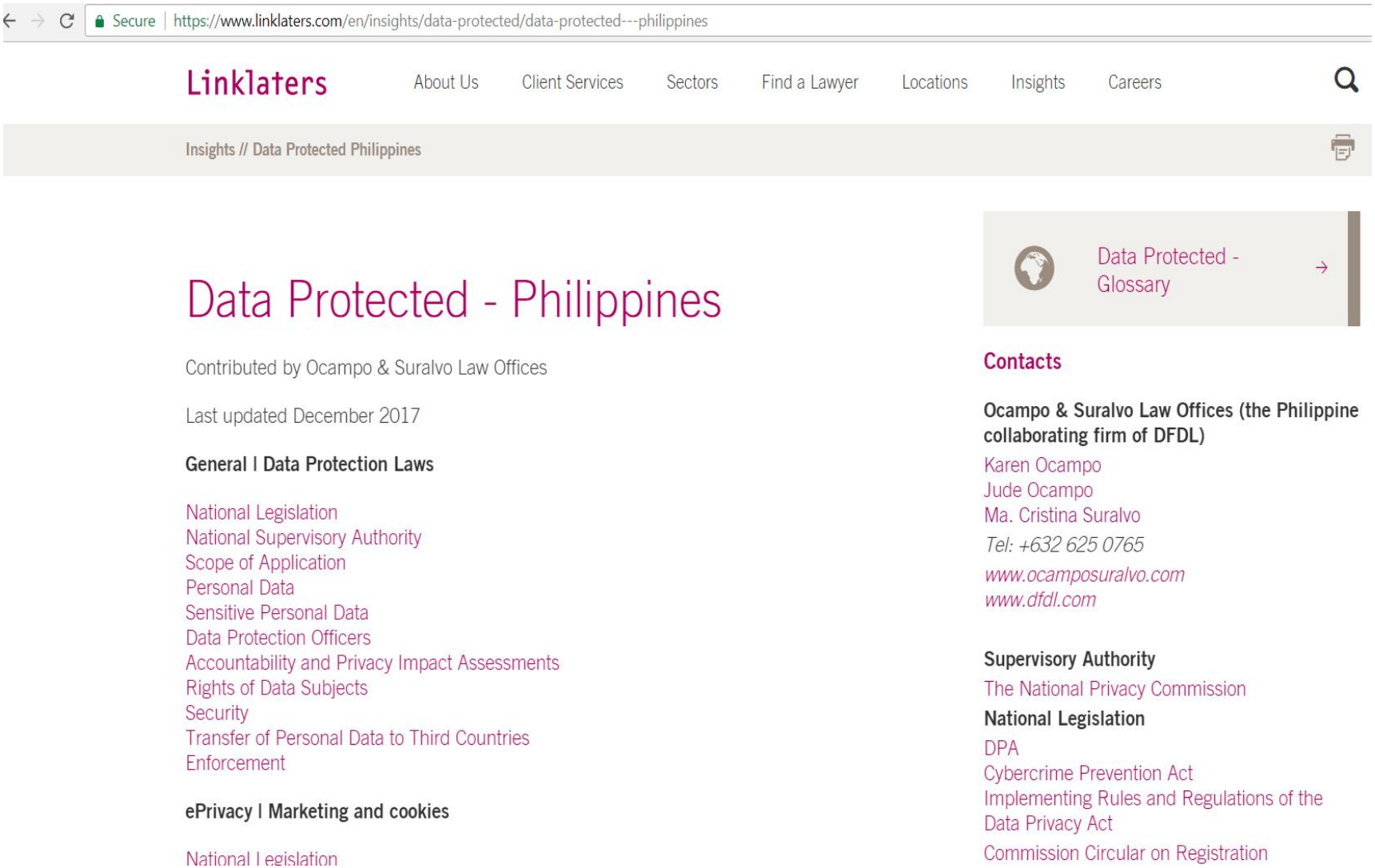
CCI-France & Philippines Netherlands Business Council

28 February 2018

OCAMPO & SURALVO

- **Ocampo & Suralvo** (OS Law) is a Philippine commercial, corporate and tax law firm. We assist clients with their legal needs across a spectrum of business concerns including corporate and commercial matters, energy, foreign investment and company establishment and registration, joint ventures, contract negotiation and drafting, mergers and acquisitions, corporate restructuring employment law, tax law and data privacy.
- OS Law is a member of the DFDL legal network.
- OS Law continues to work with international law firms to address the data privacy law concerns of their cleints' Philippine branches and subsidiaries.
- OS Law is the Philippine contributor to Linklaters' Insights *Data Protected.*

Data Privacy Resource



AGENDA

OCAMPO & SURALVO LAW OFFICES

PRIVACY	• Brief update on the Data Privacy Act (DPA)
PRINCIPLES	• Motivating principles of the DPA
PROBLEMS	• Issues and challenges in complying with the DPA
PRACTICES	• Helpful practices to allow easier compliance

OCAMPO & SURALVO LAW OFFICES

THE RULES

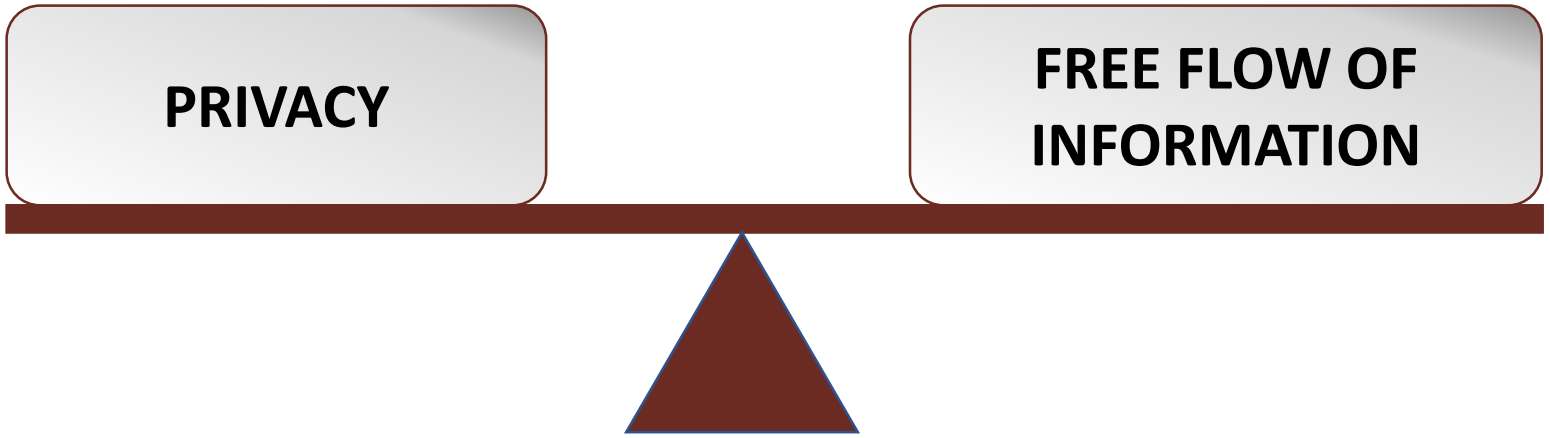
Data Privacy Act (Republic Act No. 10173)

Implementing Rules and Regulations (IRR)

Issuances of the National Privacy Commission (NPC)

OCAMPO & SURALVO LAW OFFICES

THE GOAL



OCAMPO & SURALVO LAW OFFICES

Data Privacy Act, Section 2

*It is the policy of the State to **protect the fundamental human right of privacy**, of communication while ensuring **free flow of information** to promote innovation and growth. The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.*

The Data Privacy Act: Introduction and Update

OCAMPO & SURALVO LAW OFFICES

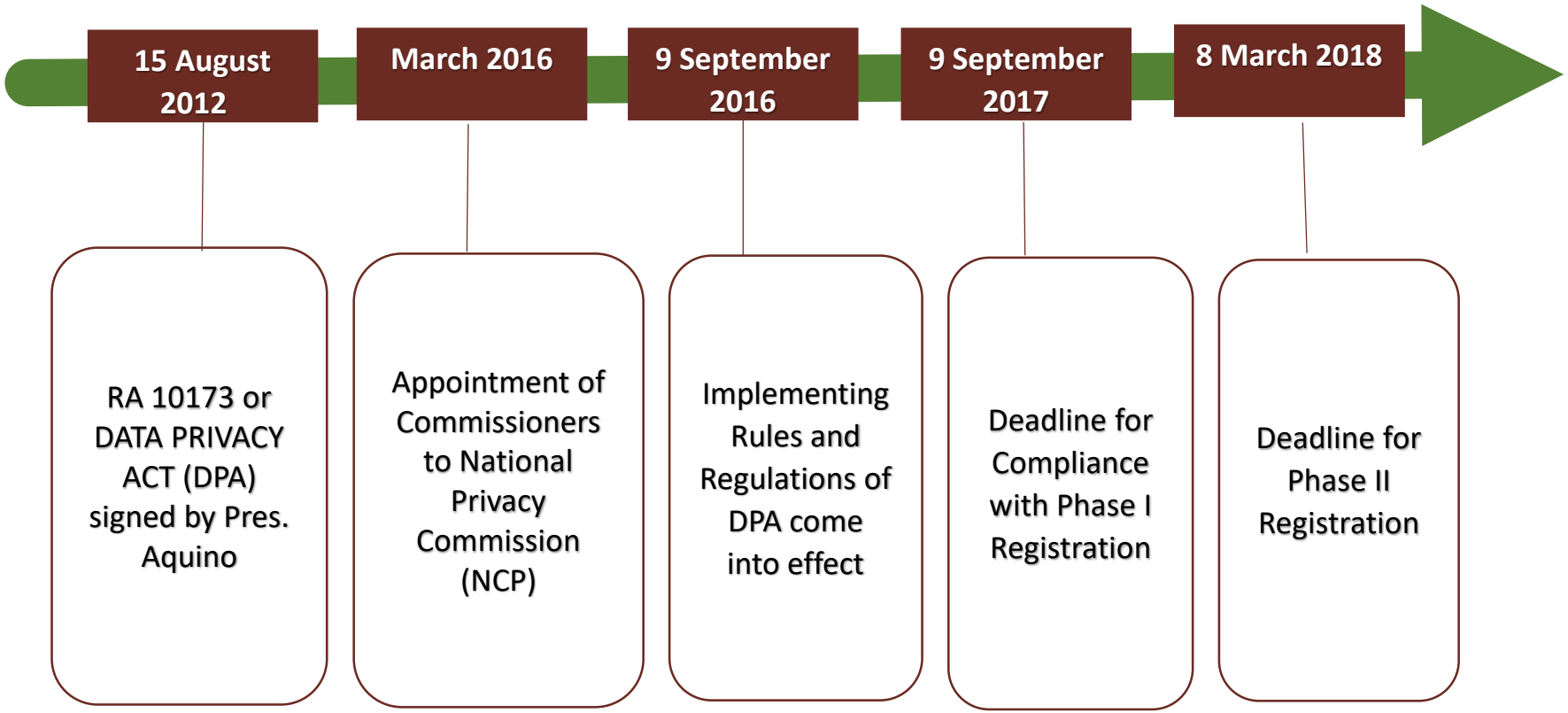
Circular 16-01	• Security of Personal Data in Government Offices
Circular 16-02	• Data Sharing (in Government Agencies)
Circular 16-03	• Personal Data Breach Management
Circular 16-04	• Rules of Procedure of the NPC

The Data Privacy Act: Introduction and Update

OCAMPO & SURALVO LAW OFFICES

Circular 17-01	• Registration of Data Processing Systems (DPS)
Advisory 17-01	• Designation of Data Protection Officers (DPO)
Advisory 17-02	• Access to Personal Data Sheets of Government Personnel
Advisory 17-03	• Guidelines on Privacy Impact Assessments (PIA)

The Data Privacy Act: Introduction and Update



- The original deadline for registration of data processing systems was 9 September 2017, which is one year from the effectivity of the IRR.

- However, while the NPC retained that deadline for the registration of DPOs (Phase 1 Registration), the deadline for the registration of data processing systems (Phase 2) was extended to 8 March 2018. *[NPC Circular 2017-01, Section 31]*

By now, you should have:

- Designated your Data Protection Officer (DPO)
- Received your access codes
- Apprised data subjects of their rights through privacy notices
- Conducted your Privacy Impact Assessments (PIA)
- Set up and cascaded your privacy policies, including your data breach management policies
- Begun registering your data processing systems with the NPC – ***8 March Deadline***
- Incorporated data privacy principles and DPA requirements in your contracts

OCAMPO & SURALVO LAW OFFICES

JARGON

Processing: any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. *[DPA, S3(j)]*

Personal Data: all types of personal information *[IRR, S3(j)]*

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 and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual. *[DPA, S3(g)]*

Sensitive Personal Information: personal information

1) about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

2) about an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

3) issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

4) specifically established by an executive order or an act of Congress to be kept classified. *[DPA, S3(l)]*

The Data Privacy Act: Introduction and Update

Personal Information Controller (PIC): refers to a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes:

1. A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or
2. A natural person who processes personal data in connection with his or her personal, family, or household affairs;

There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing *[IRR, S39(m)]*

The Data Privacy Act: Introduction and Update

OCAMPO & SURALVO LAW OFFICES

Privileged Information: any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication. *[DPA, Section 3(k)]*

Personal Information Processor (PIP): any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject *[DPA, S3(i)]*

Data Subject: an individual whose personal information is processed. *[DPA, S3(c)]*

Principles of the DPA: General

OCAMPO & SURALVO LAW OFFICES

PRINCIPLES

TRANSPARENCY

LEGITIMATE PURPOSE

PROPORTIONALITY

TRANSPARENCY

- The data subject must be aware of:
  - nature
  - purpose
  - extent of the processing (including the risks and safeguards involved)
  - identity of personal information controller,
  - his rights as a data subject
  - how rights can be exercised
- Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language. *[IRR, Section 18]*

OCAMPO & SURALVO LAW OFFICES

LEGITIMATE PURPOSE

- The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. *[IRR, Section 18]*

OCAMPO & SURALVO LAW OFFICES

PROPORTIONALITY

- The processing of information shall be:
  - adequate
  - relevant
  - suitable
  - necessary, and
  - not excessive in relation to a declared and specified purpose.
- Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.*[IRR, Section 18]*

Principles of the DPA: Processing

CRITERIA FOR LAWFUL PROCESSING

PERSONAL INFORMATION	SENSITIVE PERSONAL INFORMATION	PRIVILEGED INFORMATION
Allowed unless prohibited and when at least one of the below exists:	Prohibited except in the following cases:	Prohibited except in the following cases:
• Consent given prior to the collection or as soon as practicable and reasonable • Contractual Necessity • Legal Obligation • Vital Interests of the data subject including life and health • Public Interest or Public Authority • Legitimate Interest	• Consent specific to the purpose given prior to processing pursuant to declared, specified and legitimate purpose • Legally mandated with guarantee of protection for the information • Life and Death situation • Lawful noncommercial objectives of public organizations • Medical Treatment • Protection of Lawful Rights, Legal Claims and Provided to Government	• All parties gave consent before processing - given prior to processing pursuant to declared, specified and legitimate purpose • Legally mandated with guarantee of protection for the information • Life and Death situation • Lawful noncommercial objectives of public organizations • Medical Treatment • Protection of Lawful Rights, Legal Claims and Provided to Government

Principles of the DPA: Processing

GENERAL PROCESSING PRINCIPLES

Purpose Specification	Fair Obtaining	Accurate, relevant and up-to-date
• *collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only*	• *processed fairly and lawfully*	• *inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted*

Principles of the DPA: Processing

GENERAL PROCESSING PRINCIPLES

Adequate and not excessive	Retention Time	Form Stored
• *in relation to the purposes for which they are collected and processed*	• *only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law*	• *kept in form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed;*

Problems

CONCEPTUAL CONFUSION

PIC vs. PIP

- *Difference in Responsibility*
- *Difference in Control*
- *Difference in Form and Substance of Agreement (Data Sharing Agreement vs. Outsourcing/Subcontracting Agreement)*

Data Privacy vs. Confidentiality

- *Difference in Objectives*
- *Difference in Drafting Documentation*

Problems

PIC vs. PIP

Data Sharing Agreement

- o purpose of data sharing
- o parties to the agreement
- o term or duration of agreement
- o overview of the operational details of the sharing
- o general description of the security measures
- o how data subject may exercise its rights
- o PIC responsible for addressing requests or complaints
- o method for secure return, destruction or disposal of the shared data and the timeline therefor.

Data Processing/Service Agreement

- o Processing only upon documented instructions by PIC
- o Confidentiality obligation on authorized persons
- o Security measures
- o Prohibition against subcontracting without PIC prior instruction
- o Assisting PIC in ensuring compliance with law and regulations
- o Timely deletion or return of personal data after end of provision of services
- o Make available information necessary to demonstrate compliance (AUDITS)
- o Inform PIC if instruction violates data privacy law or regulations

Problems

Data Privacy vs. Confidentiality:

Confidentiality clauses are the wrong tools to address data privacy concerns/reqts.

The Agreement. This Confidentiality Agreement (the "Agreement") is entered into by and between ACME CORP and CYBERDYNE CORP ("Receiving Party") for the purpose of preventing the unauthorized disclosure of Confidential Information as defined below…

Definition of Confidential Information. For purposes of this Agreement, "Confidential Information" shall include all information or material that has or could have commercial value or other utility in the business in which Disclosing Party is engaged. If Confidential Information is in written form, the Disclosing Party shall label or stamp the materials with the word "Confidential" or some similar warning. If Confidential Information is transmitted orally, the Disclosing Party shall promptly provide a writing indicating that such oral communication constituted Confidential Information. The following shall not be considered as Confidential Information: information that is: *(a) publicly known at the time of disclosure or subsequently becomes publicly known through no fault of the Receiving Party; (b) discovered or created by the Receiving Party before disclosure by Disclosing Party; (c) learned by the Receiving Party through legitimate means other than from the Disclosing Party or Disclosing Party's representatives; or (d) is disclosed by Receiving Party with Disclosing Party's prior written approval…*

Obligations of Receiving Party. Receiving Party shall hold and maintain the Confidential Information in strictest confidence for the sole and exclusive benefit of the Disclosing Party….

Tips on Drafting your DPA-related Contracts

- Use Standalone or Annexed Data Sharing or Data Processing Agreements instead of embedding data privacy terms with the commercial clauses
  - Easier to amend when there are changes in law and technology
  - Ease of use for contract managers

Tips on Drafting your DPA-related Contracts

- Use the Data Sharing Agreement Circular as guide
  - NPC designed this issuance primarily for government agency data sharing BUT it has confirmed that the general conditions can be used as a guide for private agreements

Tips on Drafting your DPA-related Contracts

- Be prepared to give your foreign counterparty an explanation of the main issues and requirements of the DPA – foreign counterparties in jurisdictions which have not yet adopted modern data protection rules sometimes ask for your thoughts on these matters, especially for DSA counterparties as they themselves will need to comply with the DPA – but require them to obtain their own/separate advice from counsel (no reliance on your statements).

Tips on Drafting your DPA-related Contracts

- Ensure that the required clauses for DSAs and Service/Outsourcing contracts are included in the agreement

QUESTIONS?

OCAMPO & SURALVO LAW OFFICES

Jude Ocampo

e: jocampo@ocamposuralvo.com
t: +632 625 0765
w: www.ocamposuralvo.com
w: ph.linkedin.com/in/jbocampo

Philippine Investment Guide Download Link:
http://www.ocamposuralvo.com/publications.html