NATIONAL PRIVACY COMMISSION

Challenges in complying with the Data Privacy Act of 2012

Damian Mapa
Deputy Privacy Commissioner

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 18 February 2014

T-PD(2013)11

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (T-PD)

RECOMMENDATION R (87) 15 – TWENTY–FIVE YEARS DOWN THE LINE

by Professor Joseph A. Cannataci and Dr. Mireille M. Caruana

Executive Summary

- In order to prevent and detect crime as well as investigate and prosecute it, a law enforcement agency requires timely access to personal data. Often, this data is held by the private sector possibly in another country/in the cloud.
  - Delays in access may put human life, dignity, privacy and property at risk. Because of the huge amount of personal data that needs to be analysed quickly, this will increasingly need to be carried out in an automated way across national borders.
  - Investigators and prosecutors are faced with a constant jurisdictional issue: what precisely are the limits to their activities as they follow leads and suspects in cyberspace far across their borders into databases or user-generated content under the jurisdiction of another law-enforcement agency.
- C**onclusion**: For the automated access to be timely, it may need to dispense with ad-hoc authorization and instead rely on pre-authorization, something which can only be properly provided for across borders by binding laws.

Towards Automated Access

Adequacy Status for Police Sector

- Convention 108
- APEC CBPR

Binding Cross-Border Legal Instrument

- Add Protocol to Conv 185
- Data Sharing MLA

Adequacy Status for Police Sector

Universal Declaration of Human Rights (1948)

- European Convention on Human Rights (1953)
- Convention 108 (1981)
- Data Protection Directive (1995)
- Convention 185 (2004)
- GDPR (2018)
- Philippine Constitution (1987)
- Supreme Court ruling on Habeas Data (2008)
- Data Privacy Act (2012)
- IRR and other Issuances (2017)

Purpose of the Data Privacy Act

Purpose:

- to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth
- to ensure that personal information in information and communication systems in the government and in the private sector are secured and protected
- to create an independent body to administer and implement the Act: the National Privacy Commission

Definitions in the Data Privacy Act

Definitions (Section 3):

- Data subject
- Consent
- Personal information
- Sensitive personal information
- Personal information controller
- Personal information processor

Highlights of the Data Privacy Act

Rights of the Data Subject (Sections 16 – 18):

- Right to be informed
- Right to object
- Right to access
- Right to correct/rectify
- Right to block/remove
- Right to data portability
- Right to file a complaint
- Right to be indemnified

ECtHR Cases

- Allan v. the UK, 2002
- S. and Marper v. the UK, 2008

H

Obli

- U
- P
  p
- S
  re and
  te
- D
  a
- N
  b
- Register systems and service providers

Punishable Act	Jail Term	Fine (Pesos)
Access due to negligence	1y to 3y ☐3y to 6y	500k to 4m
Unauthorized processing	1y to 3y ☐3y to 6y	500k to 4m
Improper disposal	6m to 2y ☐3y to 6y	100k to 1m
Unauthorized purposes	18m to 5y ☐2y to 7y	500k to 2m
Intentional breach	1y to 3y	500k to 2m
Concealing breach	18m to 5y	500k to 1m
Malicious disclosure	18m to 5y	500k to 1m
Unauthorized disclosure	1y to 3y ☐3y to 5y	500k to 2m
Combination of acts	3y to 6y	1m to 5m

Who is liable?

- **Sec. 22.** The head of each government agency or instrumentality shall be responsible for complying with the security requirements mentioned herein…

- **Sec. 34.** Extent of Liability. If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime.

What happens if you don't comply?

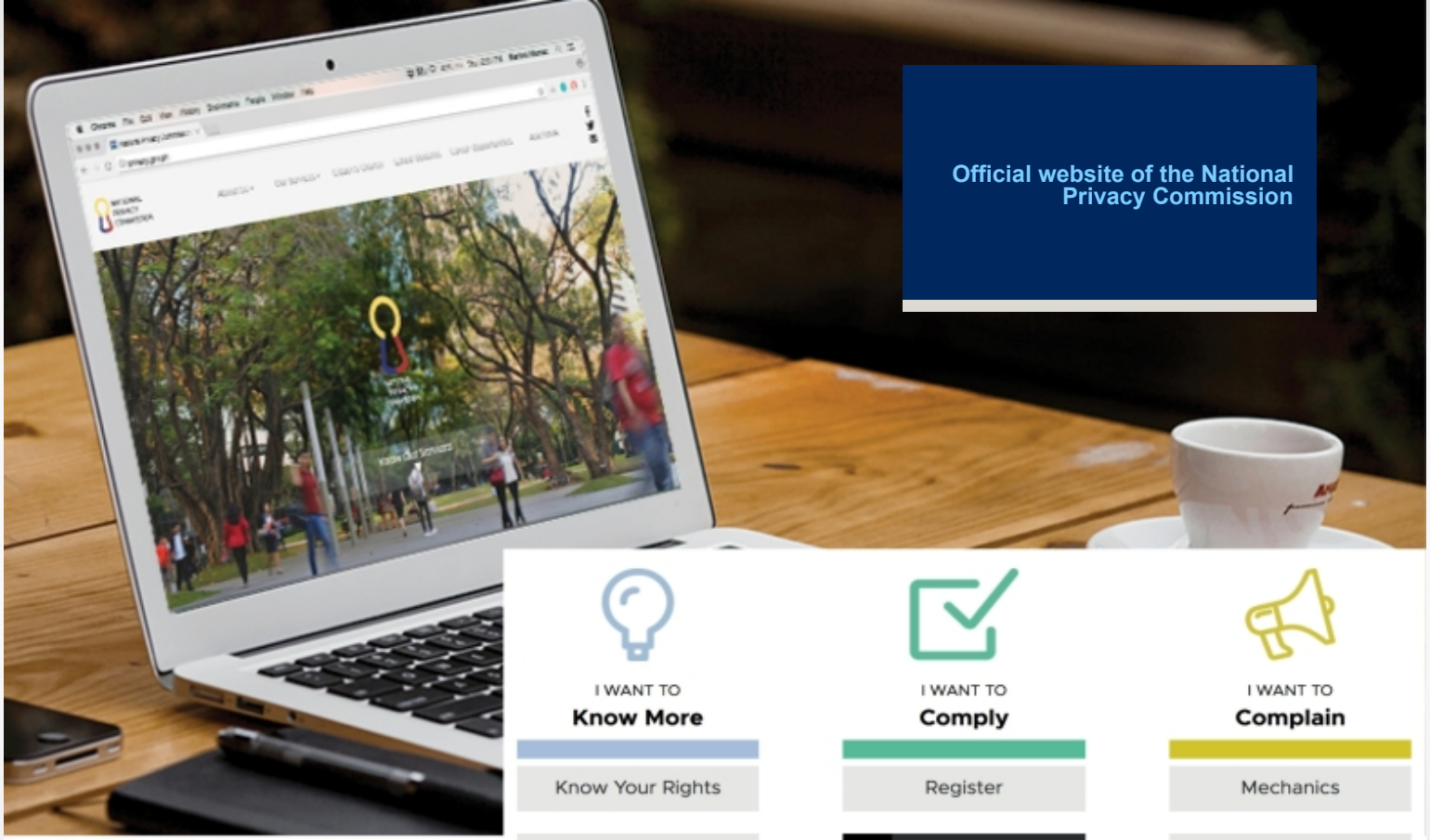
Sec. 7. Functions of the National Privacy Commission…

(b) Receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report…

(c) Issue cease and desist orders, impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest;

(d) Compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy;

(i) Recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in Sections 25 to 29 of this Act;


Official website of the National Privacy Commission
I WANT TO
Know More
Know Your Rights
The Data Privacy Act and Its IRR
Memorandum Circulars
I WANT TO
Comply
Register
Appointing a Data Protection Officer
Conducting a Privacy Impact Assessment
I WANT TO
Complain
Mechanics
Submit a Complaint
NATIONAL PRIVACY COMMISSION

Thank you!

PRIVACY.GOV.PH

facebook.com/privacy.gov.ph
twitter.com/privacyph
info@privacy.gov.ph

NATIONAL PRIVACY COMMISSION