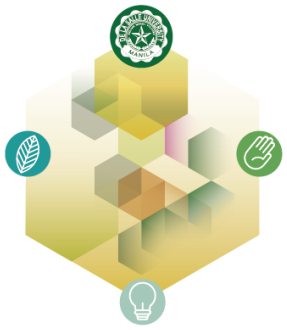
DLSU RESEARCH CONGRESS 2023
MANILA, PHILIPPINES
JULY 5-7, 2023
Fostering a Humane and Green Future:
Pathways to Inclusive Societies and Sustainable Development

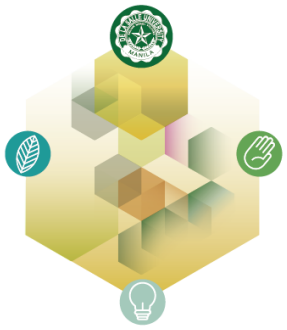


Managing Data Privacy Compliance and Technology Rollout in the Philippines post COVID-19

Danny Cheng
Information Technology Department
College of Computer Studies De La Salle University
danny.cheng@dlsu.edu.ph

Abstract: In the months and years since the publication of the IRR of the Data Privacy Act of 2012 on August 2016, the National Privacy Commission has published hundreds of circulars, advisories, and advisory opinions (NPC, 2016b). A number of these publications have direct impact on how technology use ranging from day-to-day activities such as email and social media to applications of blockchain should be sensitive to the data privacy requirements of the law and the protection of the rights of the data subject involved. Some of the publications were a consequence of the accelerated adoption of technology due to the onset of the COVID-19 pandemic the shifted lifestyle, work, and education to an online paradigm. This paper summarizes the general implications and impact of the publications to technology use through the survey and analysis of the published documents to provide general guidance on supporting data privacy to the technology sector. The commonalities and nuances of the publications impact to technology use is contrasted with the risks and benefits the use of such technology provides. After which, the paper maps them to the principles of Privacy by Design (PbD) (Ježová, 2020) to provide a recommendation to managing privacy compliance requirements in the evolving use of technology. In doing so, the paper contextualizes the PbD principles to local regulations and interpretations based on the issuances of the regulator. The paper also aims to increase the awareness of the technology sector that may eventually embed data privacy considerations into the use and deployment of technology through sample cases of privacy by design to manage technology rollout.

Key Words: data privacy; information technology; compliance; data protection; privacy by design;



1. INTRODUCTION

The recognition of the need to support the data privacy rights of individuals globally have seen a steady increase over the past decade as governments understood the value of personal data and the need to protect it for both online and offline activities to grow. This is evidenced by the number of countries and jurisdictions that have in one way or another developed data privacy or data protection regulations or are in the process of developing one (UNCTAD, 2023). At the same time, the use and deployment of technology has also been accelerated not only due to technology innovations but was further accelerated due to the COVID-19 global pandemic that created the necessity for technology adoption (Alashhab et al., 2021; Pokhrel & Chhetri, 2021). These two factors created a scenario where questions arise on how to properly deploy, adopt, and manage technology use as it not only deals with use of new technology, but also the increased volume of use of existing technology that in itself develops complexities that were previously unnoticed and not taken advantage of as in the case of videoconferencing tool adoption during the pandemic (Grant et al., 2021; Kagan et al., 2020).

This paper presents shows alignment, implications, and impact of data privacy to technology use to provide some understanding and guidance on considerations that are needed in technology adoption in the context of the Philippines by identifying common factors of consideration and discussion of cases and their resolutions. Such factors are then mapped or aligned with the Privacy by Design principles to provide structure that can illustrate how the technology sector can adapt and comply with the privacy compliance requirements as observed not just through the law but also the issuances of the regulator.

2. METHODOLOGY

2.1 Document-based survey

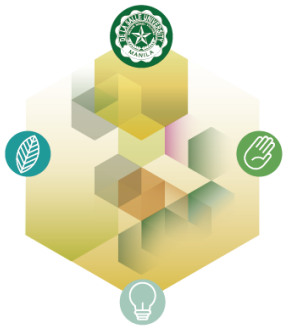
To understand the current state of privacy compliance requirements in the Philippines, the study surveyed the various issuances of the National Privacy Commission (NPC) which is the regulator tasked with enforcing the Data Privacy Act of 2012 (DPA) (Philippine Fifteenth Congress, 2012) and its Implementing Rules and Regulation (IRR) (NPC, 2016a). This is necessary to collect perspectives of the NPC as the regulator tasked with implementing the DPA. The study included the following issuances of the NPC that discusses or relates to technology use:

- Circulars – prescriptions or requirements published that went through public consultations.
- Advisories – important advice from the regulator.
- Advisory opinions – expression of opinion or legal judgement from the perspective of the regulator only as opposed to judicial decisions.

Note that technology use is not limited to enterprise systems or cutting-edge technology use such as incorporation of artificial intelligence into the processing of personal data. Technology use also includes the day-to-day use of mobile devices, social media, cameras or CCTV that the general public or data subject may take for granted. A breakdown of the number of issuances published by the NPC from 2017 to 2023 and the number of these documents that are related to technology based on the title of the document published are shown in Table 1. Other documents such as decisions, resolutions, and orders of the NPC are also considered in the study but only to the extent needed to provide additional specific cases and perspective in relation to the documents stated in Table 1.

Table 1. NPC Issuances Count by Year (Number of technology related)

Type of Document	2017	2018	2019	2020	2021	2022	2023
Circular	1 (1)	3 (0)	0 (0)	6 (3)	2 (0)	5 (4)	0 (0)
Advisory	3 (1)	1 (0)	0 (0)	5 (1)	3 (0)	1 (0)	0 (0)
Advisory Opinions	74 (6)	90 (8)	52 (4)	55 (7)	45 (6)	28 (8)	9 (0)
Total	78 (8)	94 (8)	52 (4)	66 (11)	50 (6)	34 (12)	9 (0)



2.2 Privacy by Design Principles

In order to provide structure to managing technology while aligning with privacy compliance, the study made use of the principles defined under the Privacy by Design framework (Ježová, 2020). There are seven (7) principles under the framework namely:

- Be proactive and not reactive
- Privacy as a default (Privacy by Default)
- Embedding privacy into the design lifecycle
- Providing full functionality (non-zero sum)
- Providing end-to-end security
- Providing visibility and transparency
- Respecting the users privacy

The rationale for the framework is to ensure that privacy compliance is integrated into the lifecycle as oppose to a separate activity or afterthought of the process.

2.3 Mapping Process

On mapping the privacy by design principles to the issuances of the NPC, the criteria are listed in table 2. The inclusion criteria is based on the definitions of PbD principles (Cavoukian, 2011) where they are translated to physical artifacts that are aligned with terminology used in current regulatory documents and recommendations.

Table 2. Criteria for mapping process

Principle	Inclusion Criteria
Be Proactive	Privacy Impact Assessment, Registration Process, Privacy Policy
Privacy by Default	Use of Legitimate Purpose aside from consent, anonymization, proportionality
Embedding Privacy in Design Cycle	Privacy Policy or Manual, Design Process and Considerations
Full Functionality	Use of Legitimate Purpose aside from consent, alternative processing methods
End-to-End Security	Information Security Management System, Security Controls
Visible and Transparent	Privacy policy / notice, Consent, Accessibility and being informed

3. RESULTS AND DISCUSSION

In surveying and mapping the issuances to the PbD principles (see Table 3), the following observations were made:

- Discussions of the issuances focus mainly on the regulation as would be expected and as shown in table 3 given that most documents mapped to the principles of visibility, transparency, and respect of user privacy or the data privacy rights of the data subject. These principles can be mapped directly to the privacy principles as defined in the law (Philippine Fifteenth Congress, 2012). This also shows the emphasis given by the regulator to these principles as these would be recommended starting points on the journey to privacy compliance.

- The principle with the least discussion also serves as the principle that is hardest to implement. The ability to provide full functionality as opposed to the common practice of denying access if for example consent was not given. This requires significant evaluation and reengineering of existing processes to take into account the stipulations of the law and the extent full functionality can be provided. A common cause for such conflict is the unavailability of a legitimate purpose for processing the data under section 13 of the DPA (Philippine Fifteenth Congress, 2012) for processing sensitive personal information aside from collecting consent of the data subject. Some possible changes in the processing to provide full functionality without consent includes anonymizing data collection and processing, limiting data collection and processing to processes not impacted by the lack of consent, or finding alternative methods of processing that can still achieve the desired result.

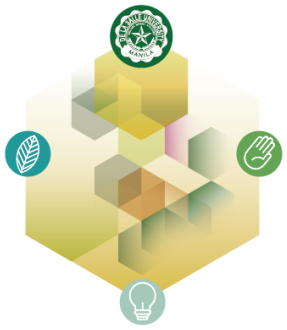


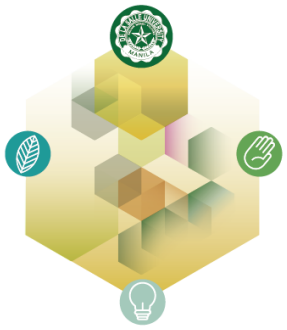
Table 3. Relating technology related issuances to Privacy by Design Principles (C-Circular, A-Advisory, AO-Advisory Opinion):(Count of document)

Principle	2017	2018	2019	2020	2021	2022	Total
Be Proactive	C:1, A:1, AO:3	AO:1		C:1, A:1		C:3, AO:4	15
Privacy by Default	AO:3	AO:3	AO:2		AO:2	C:2, AO:4	17
Embedding Privacy in Design Cycle	C:1, A:1, AO:1	AO:1		C:2, A:1		C:3, AO:2	12
Full Functionality						C:1	1
End-to-End Security	C:1, A:1, AO:2		AO:1	C:1, AO:1		C:2, AO:1	10
Visible and Transparent	C:1, A:1, AO:3	AO:3	AO:2	C:1, A:1, AO:3	AO:4	C:3, AO:6	28
Respect for user privacy	AO:1	AO:6	AO:3	C:1, A:1, AO:6	AO:5	C:3, AO:7	33

The advisory opinions (see Table 4), published by the regulator are further clustered and reviewed to gain a deeper perspective and understanding on the considerations needed for the use of specific technology. Advisory opinions are published upon the formal request by an individual or an organization to the NPC on specific matters and situations or cases. The clustering shows the common concerns of the general public requesting for opinions where most concerns are with respect the supporting the data privacy rights of the data subject, followed by the processing of camera and related recordings, and communications or marketing activities. The least amount of concerns raised relate to security both for electronic and physical information. The rationale behind the lack of concerns and opinions cannot be determined from the documents provided but some possibilities may include the existence of circulars from the regulator and industry standards that can be followed to provided details on data protection requirements. From the set of advisory opinions, a few are worth noting as they may provide unconventional opinions with respect to traditional practices such as monitoring of computers and devices issued by the company, the ability confiscate devices by a teacher from the student, the process of forensic investigation, and posting of photos of in social media without consent.

Table 4. Available Advisory-Opinions grouped into themes showing technologies considered.

Themes	Relevant Advisory Opinions
Camera and Recordings	1. Use of Body-Worn Camera by Security Personnel 2. Use of Camera During Surveillance Visits 3. Recording and Uploading of Online Classes 4. Disclosure of Screenshots of a Private Conversation 5. Use of Body-worn Camera Pursuant to a Pea tollway Corporation Policy 6. Processing of CCTV footage under the data privacy act of 2012 7. Viewing and/or release of CCTV footage
Data Protection	1. Disclosure of Personal Information for Cybersecurity Investigations 2. Forensic Audit on Company-issued Assets and Company-related Accounts 3. Use of Blockchain Technology for the Philippine Personal Property Security Registry 4. Storage and sharing of electronic medical records (EMR)
Rights of the Data subject	1. Posting of Photo in a Social Media Platform Without Consent 2. Online Lending Mobile Application Permissions



	3.	Remedies Against the Alleged Data Breach Involving Workabroad.ph
	4.	Processing of Personal Data Contained in Abandoned Servers or Computers
	5.	Data Subject Rights in the Philippine Identification System
	6.	Processing Personal Data for Electronic Know-your-customer (eKYC)
	7.	Deletion of Electronic Medical Records
	8.	Right to Delete Account Through E-mail
	9.	Data Privacy and office-issued mobile devices
	10.	Computer monitoring
	11.	Access to medical records in CR-DR system
	12.	Teachers' right to search a minor students cellular phone
Physical Data and Physical Security	1.	Transport of Physical Media Containing Personal Data
	2.	Facial Recognition for Id System
Communication and Marketing	1.	Legality of Spamming and its Effects on Data Privacy
	2.	Mass Email Sent using Carbon Copy
	3.	Use of Pop-Ups for Information on the Use of Cookies
	4.	Anonymized data for marketing analytics
	5.	Reverse Search Module

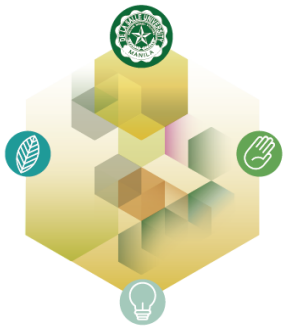
4. CONCLUSIONS

The results show how the issuances of NPC maps to the PbD principles and the principles that is given emphasis by the regulator. The deeper review of the advisory opinions also showed alignment with the prioritized PbD principles and the clustering of advisory opinions. This can provide a roadmap to institutions who are using or deploying technology solutions on which areas to prioritize namely start with transparency and rights, then register and conduct impact assessments, after which ensure data protection and finally embed in organizational process and proceed to process reengineering. Though this may not be ideal, prioritization is important given that change and compliance will not happen immediately and limited resources needs to be managed and optimized in terms of their utilization. The results also show that the publications or issuances of the NPC can serve as a valuable resource for guidance on needed considerations when managing technology deployment.

One notable observation is that the privacy principle of transparency does not equate to collection of consent as some of the opinions considers the use of alternative and appropriate legitimate purposes aside from consent. Proportionality can also be used to reduce or limit the necessity to collect consent. The rationale for prioritizing other legitimate purposes and proportionality is that consent can be revoked, or objected to, or be declared invalid when challenged. Another observation is that some of the opinions do not provide clear suggestions as the details in the request for an opinion might be limited or the technology may be relatively new such as the use of Facial Recognition for ID Systems where the opinion cited the legitimate purpose for processing personal data but did not further elaborate on the use of facial recognition technology for the stated and even related purposes. Such observations show that there is still plenty of room for discussion and recommendation of practices as technology and the regulation evolves over time and changes in either one can create significant implications on how data privacy can be respected and implemented with respect to use of technology and personal data.

5. RECOMMENDATIONS

The study is currently limited to issuances that are technology related or contains explicit discussion or reference to use of technology. However, it was observed during the course of the study that there are other issuances that do not refer specifically to technology use that can be eventually used as guidance on technology related deployment. An example would be issuances that discuss specifically about the data privacy rights of the data subject. Rights would apply whether or not technology is involved in the processing of personal data. As such,



these documents can be included in future studies to provide more insights on how privacy compliance can be managed in relation to technology deployment. Another recommendation would be to provide a more granular study of the issuances to provide detailed cases or guidance for each PbD principle and consider the current gaps in the issuances such as the principle on providing full functionality or non-zero sum. The more granular study can also be used to further cluster opinions and decisions to possibly extract practice recommendations that can be applied to other forms or cases of technology use to allow for a more responsive approach to data privacy compliance and governance. Possible tiering can also be developed to consider the different states of institutions and organizations in the capability to implement certain practices with respect to the resources and environment that the organizations find themselves in.

6. REFERENCES

Alashhab, Z. R., Anbar, M., Singh, M. M., Leau, Y.-B., Al-Sai, Z. A., & Abu Alhayja'a, S. (2021). Impact of coronavirus pandemic crisis on technologies and cloud computing applications. *Journal of Electronic Science and Technology*, *19*(1), 100059. https://doi.org/https://doi.org/10.1016/j.jnlest.2020.100059

Cavoukian, A. (2011). *Privacy by design in law, policy and practice. A white paper for regulators, decision-makers and policy-makers*. Retrieved from https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

Grant, M., Kennedy, J., Zhu, J., Tan, J., Markovski, S., & Popa, C. (2021). *Videoconferencing Privacy and Security Concerns in the Pandemic*.

Ježová, D. (2020). Principle of Privacy by Design and Privacy by Default. In (pp. 127-139). https://doi.org/10.18485/iup_rlr.2020.ch10

Kagan, D., Alpert, G., & Fire, M. (2020). *Zooming Into Video Conferencing Privacy and Security Threats*.

Implementing Rules and Regulations of Republic Act No. 10173, Known as the "Data Privacy Act of 2012", (2016a). https://www.privacy.gov.ph/wp-content/uploads/IRR-of-the-DPA.pdf

NPC. (2016b). *National Privacy Commission*. https://www.privacy.gov.ph/

An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, creating for this purpose a National Privacy Commission, and for other purposes, (2012). https://www.privacy.gov.ph/wp-content/uploads/DPA-of-2012.pdf

Pokhrel, S., & Chhetri, R. (2021). A Literature Review on Impact of COVID-19 Pandemic on Teaching and Learning. *Higher Education for the Future*, *8*(1), 133-141. https://doi.org/10.1177/2347631120983481

UNCTAD. (2023). *Data Protection and Privacy Legislation Worldwide*. Retrieved January 23 from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide