I am delighted to welcome you to the first issue of the Data Privacy Forum, a bimonthly newsletter for the Data Protection Officer (DPO) community in the Philippines, published in PDF format by the National Privacy Commission (NPC).

Available via email to DPOs like you, who are registered with the NPC, this newsletter is aimed at keeping you on track of the latest updates and emerging issues in the data privacy front, thus help you in getting your organization on top of its compliance obligations.

I hope you enjoy reading each issue of Data Privacy Forum. This publication is for you, so if you have a suggestion for an article or if you are interested in sharing any insights, just let us know. Your comments and feedback would also be much appreciated. This would help us ensure that this newsletter serves the DPO community in the best way possible.

As always, if there is anything the NPC can do to help in your job as DPO, do not hesitate to get in touch with us.

Thank you.

Raymund Enriquez Liboro
Privacy Commissioner and Chairman

A message from the Privacy Commissioner

Table of Contents

A message from the Privacy Commissioner .......................................................... 3
A quick look back on June and July 2017 ............................................................... 4
Roadshow Updates ............................................................................................... 6
DPO of the Month ................................................................................................. 8
The World on Privacy ............................................................................................ 10
Preparing for GDPR Compliance ..................................................................... 12
Best Practices for DPOs & Privacy-Minded Organizations ............................ 14
Updates from the Compliance and Monitoring Division ............................... 16
Updates from the Privacy Policy Office ............................................................. 18
Registered Organizations .................................................................................. 19
Upcoming DPO Events ..................................................................................... 20

The DPO Newsletter is produced by the National Privacy Commission’s Public Information and Assistance Division, with the contributions of its Privacy Policy Office, Compliance and Monitoring Division, and Complaints and Investigations Division.
A quick look back
JUNE - JULY 2017 EVENT HIGHLIGHTS

Throughout the months of June and July 2017, representatives from the National Privacy Commission served as speakers and resource persons for a number of local and international events.

Got an event you would like to invite us to? Interested in having us over to discuss more about the Data Privacy Act (DPA)? Send us an e-mail at info@privacy.gov.ph.

01

Launches

— Securities and Exchange Commission Executive-Level Briefing on the DPA
— DPA Compliance and the Fight Against Cybercrime Conference
— DPA Awareness on the DPA
— DLSU CEShout: Online Privacy Protection
— Commission on Audit Orientation on the DPA and its Implementing Rules and Regulations

02

1. June — Globe Telecom Inc. Seminar on the DPA
2. June — NeoEXM Seminar on the DPA
3. June — NEDA Orientation on the Privacy Impact Assessment
4. June — TESDA Planners’ Conference
5. June — House of Representatives Information and Communications Technology Committee Technical Working Group Meeting
6. June — Office of the President Knowledge Sharing Exercise: Laying down the foundations of Data Privacy
7. June — Aboitiz Equity Ventures (AEV) DPA Awareness and Workshop on the Conduct of the Privacy Impact Assessment
8. June — Adamson University Awareness on the DPA
9. June — FOI Conference with the Presidential Communications Operations Office
10. June — Department of Health Office for Health Service Development Cluster Orientation on the DPA and its Implementing Rules and Regulations
11. June — Banco De Oro Orientation on the DPA
12. June — ASEAN 2017 Dialogues
14. June — The Big Story Live Interview on the BPI Breach
15. June — ASEAN 2017 Dialogues
16. June — Internet and Mobile Marketing Association of the Philippines General Membership Meeting
17. June — Philippine National Bank Briefing on the DPA
18. June — Bureau of Jail Management and Penology 2nd Quarter Management Conference
19. June — Aboitiz Equity Ventures (AEV) DPA Awareness and Workshop on the Conduct of the Privacy Impact Assessment
20. June — The Big Story Live Interview on the BPI Breach
21. June — Office of the President Knowledge Sharing Exercise: Laying down the foundations of Data Privacy
22. June — Department of Health Policy and Administration’s Executive Course
23. June — Department of Information and Communications Technology Project Launching

— Securities and Exchange Commission Executive-Level Briefing on the DPA
— DPA Compliance and the Fight Against Cybercrime Conference
— DPA Awareness on the DPA
— DLSU CEShout: Online Privacy Protection
— Commission on Audit Orientation on the DPA and its Implementing Rules and Regulations

12 July — 2017 Annual Home Development Mutual Fund Lawyers’ Conference: The Lawyer as an Advocate of Data Privacy
13 July — Lyceum Polytechnic University of Manila Total Quality Instruction Development Program
14 July — Professional Regulation Commission (PRC) Seminar-Workshop
15 July — Data Privacy Asia with the Contact Center Association of the Philippines
— Harophil Seminar on the DPA
16 July — #CyberSafePH: CICC Cyber Security Caravan
17 July — Panel Discussion during the 19th founding anniversary of National Telehealth Center
PrivaMoves Roadshows

OVER THE PAST FEW MONTHS, representatives from the NPC have gone to several key cities across the country to talk about compliance with the Data Privacy Act and awareness on information privacy.

- **26 January, Cebu City**
  - In coordination with the Cebu Educational Development Foundation Technology, the ICT Association of Cebu, and the Department of Information and Communications Technology, and the Cebu Provincial Capitol
  - 78 Participants

- **01 March, Cagayan de Oro City**
  - In coordination with the ICT Association of Cagayan de Oro, the Department of Information and Communications Technology, and the Local Government of Cagayan de Oro
  - 93 Participants

- **03 March, Butuan City**
  - In coordination with the Department of Information and Communications Technology
  - 100 Participants

- **24 March, Zamboanga City**
  - In coordination with the Department of Information and Communications Technology
  - 213 Participants

- **13 May, Dumaguete City**
  - In coordination with the ICT Association of Dumaguete, National ICT Confederation of the Philippines, and Globe Business
  - 56 Participants

- **16 May, Iloilo City**
  - In coordination with the Department of Information and Communications Technology
  - 120 Participants

- **21 July, Dagupan City**
  - In coordination with the Department of Information and Communications Technology
  - 100 Participants

- **21 July, Quezon City**
  - In coordination with the Department of Information and Communications Technology and the Cybercrime Investigation and Coordination Center
  - 1,200 Participants

- **25 July, Legazpi City**
  - In coordination with the Department of Information and Communications Technology, the Albay ICT Association, Inc., Albay Chamber of Commerce, and Industry, National ICT Confederation of the Philippines, and the Local Government of Albay
  - 40 Participants

- **27 July, Davao City**
  - In coordination with the Department of Information and Communications Technology, the Cybercrime Investigation and Coordination Center, and Ateneo de Davao University
  - 668 Participants

- **29 July, Zamboanga City**
  - In coordination with the Department of Information and Communications Technology
  - 370 Participants

- **11 August, Cagayan De Oro City**
  - In coordination with the Department of Information and Communications Technology, National Telecommunications Commission, Palo Alto Networks, FireEye Singapore Private Ltd, and IECEP-Northern Mindanao Chapter
  - 2,219 Participants

Where do you think Priva should go to next? For invites, call (02)565-9623 or e-mail us at info@privacy.gov.ph.
DPO of the Month:
Leah Camilla R. Besa-Jimenez

AS THE CHIEF DATA PRIVACY OFFICER of the PLDT Group of Companies, Leah has a lot on her hands — and that is an understatement. We sat down with her for an afternoon to talk about her experiences thus far in data privacy, and what role do you think DPOs play in combating these challenges?

I think it’s all about raising the level of consciousness of the value that data provides, both as a consumer — the value my data brings to a company — and as a business person — the value the company sees in the data of the customer. As to how to build a culture of data privacy, will still be alive in the time it’s actually there? (Laughs). Commissioner Liboro said in DPO3, that the TelCos are vanguards of data privacy, and it’s true when you think about it, because we handle so much data. So my office contributes to it, I think, is not just to ensure compliance, but to establish good governance for the data that we have. Because the way we see it, protecting data is equivalent to making sure that we provide the best customer experience, which any company would be looking for, and any customer should expect, and all of this really boils down to trust. So I think our contribution, as the Data Privacy Office of the PLDT Group, is basically ensuring that the millions and millions of customer data that we have, we protect.

You have been working on Data Privacy for over a year now. Do you have any words of advice for aspiring DPOs?

I’m actually quite surprised that, according to Commissioner Liboro, a lot of people are struggling with data privacy. That’s because when we saw the IRR, we thought it was crystal clear. It’s so clear with very little room for interpretation. The difference I think with the PLDT Group implementation was very strong Senior Management support — that spelled a huge difference.

I think other people might be overanalyzing it, when I think it’s as a negative, because it’s another layer that you need to comply with. But if you think about it again, if the objective is excellent customer experience and making sure your customers trust you, then the IRR is a part of that. It has to be a given, not just something that is imposed by the government. It’s good that it’s a law with clear IRRs, of course, and the sanctions only give more teeth to the act and provide more urgency to get things done.

For any company, privacy and security really have to be baked in, it’s part of everything you do, and is not just a “by the way.” It’s not easy, but it’s also not unreasonable.

Where do you see privacy and DPOs in the Philippines 10 years from now?

Well, I’m optimistic that as everyone embraces what digital promises businesses in terms of growth, privacy should go hand-in-hand with that if you look at it from a transformation standpoint. Security is a pillar, Customer Experience is also a pillar, and the DPA affects both. So if companies seek growth in digitizing their businesses, then privacy is part and parcel of it all, something that is baked into our processes from the very beginning, up to the finished products and services.

As for DPOs in the Philippines, I think anyone working in data privacy, especially during this stage — because it’s all about setting up, and really evaluating a lot of processes — would be highly marketable. But more than that, I think there’s actually a great opportunity for them, particularly in the context of Southeast Asia, in carving the way for a more enhanced framework — something like the GDPR in Europe, but from the perspective of emerging markets. Because the Philippines is at the forefront in ASEAN to embrace data privacy, I think that the country stands a good chance of spearheading the best practices in the region. That would be an interesting move for the NPC and we’ll be here to support them.
On Ransomware
As of press time, the world has barely begun to recover from the effects of WannaCry and Petya—global ransomware attacks that have infected nearly half a million PCs worldwide. Although not an entirely new phenomenon, the attacks have only gotten more advanced and more vicious over the years, with ransomware costing institutions an estimated $1 billion in 2016 alone.

While there is no foreseeable end to these attacks, there are some steps your organization can take to avoid or alleviate the effects of ransomware. Data, as experts and observers say, is now the new oil; it thus makes sense that individuals and groups across the globe will be willing to do anything, legally or otherwise, to get their hands on it. Therefore, it even makes more sense for institutions to invest in data protection and data privacy.

The price of innovation
Last month, Google’s DeepMind ran into legal trouble after obtaining data from the Royal Free NHS Foundation Trust in the United Kingdom without the consent of its patients. While the health institution had passed its patients’ data to Google as part of a project testing an alert, diagnosis, and detection system for acute kidney injury, it DeepMind accessed this data in a manner that UK’s National Data Guard Dame Fiona Caldicott called “legally inappropriate.”

The resolution filed by the UK Information Commissioner’s Office was accepted by both camps, and better, more privacy-minded solutions are in development for the Google project. Across the Atlantic, however, rages a fiercer legal battle over data protection and privacy in the face of police surveillance and counterterrorism measures.

The New York Police Department has been sued for refusing to release information about its use of facial recognition software, predictive policing software, x-ray vans, and mosque-raking programs that violate the privacy of thousands of individuals, most especially minority communities in the City of New York. This has been the status quo despite existing Freedom of Information Laws, but the absence of regulations governing police use of facial recognition software has raised eyebrows and tensions in the city, especially among those versed in Privacy Law. Research indicates that roughly half of American adults are enrolled in face recognition networks, but very few agencies have instituted “meaningful protections to prevent the misuse of the technology.”

Benjamin Franklin once famously said that “he who sacrifices liberty for security deserves neither.” While this may be true, the global discourse on the sacrifices we make for innovation, development, and ease of interconnectivity is now becoming mainstreamed. What information is to be used, and how, and to what extent? These are questions that should ignite meaningful conversations—and it must begin with personal information controllers and processors, whose legal obligations include transparency with the information they collect and process.

This is where privacy by design comes in, guided by your Privacy Impact Assessments and outlined in your Privacy Manuals and privacy and data protection measures.

The final countdown: 10 months to GDPR
The EU Global Data Protection Regulation is set to officially kick in by 25 May 2018. Ready or not, institutions all over the globe have to comply. Is your organization ready?
Preparing for GDPR Compliance

THE EU GENERAL DATA PROTECTION REGULATION (GDPR) is a new regulation that will harmonize data protection laws across EU, replacing existing national data protection rules. Although it will not take effect until May 25, 2018, it is critical that preparation for compliance commence early to effectively implement the new obligations imposed.

Some Philippine businesses covered by the Data Privacy Act of 2012 (DPA) may need to comply with the GDPR if they:
— have an establishment in the EU (regardless of whether they process personal data in the EU) or
— do not have an establishment in the EU, but offer goods or services, or monitor the behavior of individuals in the EU.

There are similarities with the GDPR and the DPA. You would note that the DPA is largely based on the 1995 EU Directive, which is the predecessor of the GDPR. For additional resources and information, you may review the following European Commission, Reform of EU data protection rules and the Article 29 working group GDPR guidance.

EU GDPR

Scope
Personal data – any information relating to an identified or identifiable person. [Art. 4(1)]

Accountability and governance
Controllers generally must:
— Implement appropriate technical and organizational measures to demonstrate GDPR compliance and build in privacy by default and design. [Art. 5(2), 24, 25]
— Undertake compulsory data protection impact assessments. [Art. 35]
— Appoint data protection officers. [Art. 37]

Consent
Consent must be:
— Freely given, specific, informed, and unambiguous indication of data subject’s agreement to processing
— Through statement or clear affirmative action. [Art. 4(1)]

Data Breach Notification
Mandatory by controllers and processors (exceptions apply) within 72 hours of becoming aware of the breach [Art. 33-34]

Rights
Expanded individual rights include:
— Right to erasure. (Art. 17)
— Right to restriction of processing. (Art. 18)
— Right to data portability. (Art. 20)
— Right to object. (Art. 21)

Overseas transfer of personal data
May be transferred outside the EU in limited circumstances including:
— To countries that provide an adequate level of data protection
— Where standard data protection clauses or approved binding corporate rules that enable transfers within a corporate group apply
— Approved codes of conduct or certification in place. [Chapter V]

Registration of Data Processing Systems
No requirement but must maintain internal records of processing activities [Art. 30]

Sanctions
Administrative fines of up to 20 million euros or 4% of annual worldwide turnover, whichever is higher. [Art. 83]

DPA

Scope
Personal Information, Sensitive Personal Information, and Privileged Information. [Sec. 4(g), (l) and (k)]

Accountability and governance
PICs and PIPs generally must:
— Implement organizational, physical, and technical security measures. [Sec. 20]
— Conduct a Privacy Impact Assessment for each program or process that involves personal data [see, Sec. 20 and Sec. 4, NPC Circular No. 16-01]
— Appoint data protection officer/s [Sec. 21(b)]

Consent
Consent must be:
— Freely given, specific, informed indication of will that the data subject agrees to processing
— Evidenced by written, electronic or recorded means. [Sec. 3(b)]

Data Breach Notification
Mandatory by PIC within 72 hours from knowledge or reasonable belief of occurrence of the breach (exceptions apply) [Sec. 20(f)]

Rights
Same rights of the data subject except right to restriction (Sec. 16-18)
Rights are also transmissible (Sec. 17)

Overseas transfer of personal data
Recognized under the DPA; PICs still responsible for personal data whose processing is outsourced or transferred internationally [see: Sec. 6 and 21, DPA; Sec. 50, IRR]

Sanctions
Both fine and imprisonment forPICs and PIPs who meet the criteria [Sec. 46-47, IRR]
Best Practices for DPOs and Privacy-Minded Organizations

NPC CIRCULAR 16-01, which discusses the security of personal data in government agencies, mandates all organizations in the public sector to establish a control framework to address the risks identified upon the conduct of a privacy impact assessment.

Section 6 of NPC Circular 16-01 defines the control framework as “a comprehensive enumeration of the measures intended to address the risks, including organizational, physical and technical measures to maintain the availability, integrity and confidentiality of personal data and to protect the personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.”

A control framework shall take into account, among others, the items illustrated to the right.

With the continuing rise of data privacy awareness, public and private organizations across the globe are now strengthening their respective control frameworks with more stringent security measures to ensure the protection of the personal data they process. The following describe security measures considered to be best practices as implemented by PICs across the board.

1. Security Clearances

As an organizational measure, the issuance of security clearances by the Human Resources Department of a PIC is considered not only a best practice, but also a requirement for government agencies as per Section 9 of NPC Circular 16-01.

Security clearances ensure that only duly authorized personnel are allowed to process personal data collected and stored by the organization, while allowing the organization to have more control over who can view or access the personal data it stores.

In most organizations, access to information is usually determined in accordance with an employee’s functions. This means that if the personal data is not relevant or necessary in the performance of an employee’s core functions, then he or she should not have access to any personal data, regardless of his or her position in the organizational hierarchy.

2. Access Control Systems

Setting up an access control system is considered an effective security measure for any public or private organization that processes personal data, as it allows the effective recording of when, where, and by whom an organization’s data centers are accessed. As a physical measure, this is usually manifested in the form of biometrics technology as an entry/exit point in offices where personal data is being processed.

3. Privacy Notices

An indispensable part of any organization’s privacy management program is the posting of a privacy notice to its data subjects. The privacy notice serves to inform clients of what personal data will be collected and why, how long the personal data will be retained, which organizations the personal data will be shared with, and how the personal data will be disposed of, among others. The privacy notice posted on the PIC’s website or office premises promotes the data processing principles of transparency, legitimate purpose and proportionality, because they inform the data subjects how and why their personal data is being processed by the PICs. Also, it lifts the veil of ambiguity in the terms by which a data subject and personal information controller transact, because the data subjects are made to better understand the PIC’s functions in relation to their personal data.
Updates from the Compliance and Monitoring Division

THE COMPLIANCE AND MONITORING DIVISION is the NPC’s arm for ensuring compliance of personal information controllers (PICs) and processors (PIPs) in the Philippines to ensure the effective implementation of the Data Privacy Act of 2012. Its main initiative for the first few years of the effectivity of the law and its Implementing Rules and Regulations is to create and develop the registration process for PICs and PIPs. In this regard, this is the status of registration, by the numbers, as of 14 August:

<table>
<thead>
<tr>
<th>Entity</th>
<th>Actual</th>
<th>Target</th>
<th>Achieved Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>NGAs</td>
<td>119</td>
<td>61 (Executive Offices)</td>
<td>42.62% (Executive Offices)</td>
</tr>
<tr>
<td>Private Companies</td>
<td>194</td>
<td></td>
<td></td>
</tr>
<tr>
<td>State Universities and Colleges</td>
<td>70</td>
<td>112</td>
<td>62.50%</td>
</tr>
<tr>
<td>Total</td>
<td>383</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The NPC has been active in reminding the remaining offices and institutions to comply, as the deadline of registration is on 9 September 2017. For more information, visit register.privacy.gov.ph

Updates from the Privacy Policy Office

CONSIDERED AS THE KNOWLEDGE CENTER of the National Privacy Commission (NPC) that establishes data privacy and protection rules and guidelines, the Privacy Policy Office (PPO) spearheads the development of policies, advisory opinions, and standpoints on proposed legislations affecting personal data. It also provides clarifications on the interpretation of the Data Privacy Act of 2012 (DPA) and its Implementing Rules and Regulations (IRR) and other data privacy issues and concerns.

32 Advisory Opinions
These are made in response to inquiries from different stakeholders on a variety of topics. Most common of these are concerns on automated processing and decision-making, consent, data sharing, the Data Protection Officer, and exemptions in relation to existing related laws, among others.

2 Advisory Opinions
For the proper guidance of concerned stakeholders, the following advisories were produced and made available:
— Designation of a Data Protection Officer
— Access to Personal Data Sheet of Government Personnel

2 Position Papers
Position papers provide comprehensive discussion and recommendations on key issues through the lens of personal data protection, with two released recently:
— International Telecommunication Union (ITU) – Department of Information and Communications Technology (DICT) Big Data Pilot Study
— Online and Social Media Membership Accountability Act

What’s in the works for the PPO?
1. Research on the use of CCTVs, drones, and dashcams, and their privacy and data protection implications
2. An advisory on Privacy Impact Assessment (PIA) Guidelines
3. A circular on the Registration of Data Processing System, or Phase Two of PIC registration with the NPC.
Interested DPOs may RSVP with the Commission on Higher Education via e-mail at chedncr@ched.gov.ph or call (02) 441-0985 / (02) 441-1224.
DPO Briefings

Want to learn more about compliance with the Data Privacy Act but not sure where to start?

Beginning this month, we’ll be holding bi-monthly DPO Briefings at the Audio Visual Room of the Department of Information and Communications Technology Headquarters in Quezon City.

There will be morning and afternoon sessions on 16 and 30 August 2017. Organizations may reserve up to three slots for their representatives by calling our office at (02) 565-9623 today or sending an e-mail to paola.nartea@privacy.gov.ph.

WANT YOUR SECTOR to be front and center in the next DPO Assembly? Send us an e-mail at info@privacy.gov.ph.
3rd Floor, Core G, GSIS Headquarters Bldg.,
Financial Center, Pasay City, Metro Manila 1308

For invitations: (02)565-9623
For complaints: (02)517-7806
For compliance: (02)517-7810
For public assistance: 09451534299 / 09399638715

privacy.gov.ph
privacyPH
info@privacy.gov.ph
complaints@privacy.gov.ph

#AskPriva #PrivacyPH