Checklist for Data Protection Officer (DPO)

Within 30 days:

- ☐ Draw up your TOR. Be sure to get an assurance that you shall be reimbursed in case of litigation related to the Data Privacy Act.
- ☐ If your organization is considered medium- or high-risk, you may want to consider forming a data protection task force or committee, or at the least, having an assistant DPO.
- ☐ Register your appointment/designation with the NPC, likewise, update organization's website to reflect such.
- ☐ Join an existing network of privacy professionals, such as the IAPP (International Association of Privacy Professionals). Or organize one yourself, perhaps your industry association could have a special interest group for DPOs.
- ☐ Reach out to your counterpart in a similar organization in Europe, Canada, Australia or the US. He or she can coach you about the role, and can share their best practices.
- ☐ Send out an RFQ for an external consultant to do an IT Security audit to discover what are your organization's "pre-existing conditions".
- ☐ Send out an RFQ for a software application to assist you in monitoring compliance of the organization. These tools should include features such as workflow management, and document management.
- ☐ Obtain an organizational inventory of processes that handle personal data, including the list of process owners.

Within 90 days:

- ☐ Acquire and deploy a software application to assist you in monitoring compliance of the organization. These tools should include features such as workflow management, and document management.
- ☐ Develop your own plan for continuing education and consider working towards a certification such as IAPP's CIPT and CIPM certifications.
- ☐ Schedule workshops with all process owners to do a Privacy Impact Assessment (PIA) of the process/es which they own.
- ☐ Use the results of the PIAs to begin drawing up your organization's control framework for privacy and data protection.
- ☐ Select an external consultant to conduct an IT Security audit, and initiate such audit.
- ☐ Establish a breach management framework for the organization.

Within 180 days:

- ☐ Review results of IT Security audit with top management.
- ☐ Ensure that all those who are handling personal data have been issued a security clearance by the head of organization.
- ☐ With the help of HR, Legal, IT, and Security, begin drafting your organization's privacy and data protection policies. If your organization handles personal data for more than 1,000 individuals, NPC recommends the use of the ISO/IEC 27002 control set as the minimum standard to assess any gaps in your control framework.
- ☐ Select a governance framework that will help you strategize and orchestrate the implementation of the organization's privacy programs. There are several available, and you may want to start with a simple one. Within 12 to 18 months, you can then assess whether you need to evolve to a more advanced framework. This is consistent with an approach of continuous assessment and development, taking into account inputs from top management and the process owners.
- ☐ Conduct breach management drill/s, prioritizing those processes with the highest privacy risk.

Checklist for CEO/Head of Agency

Within 30 days:

- ☐ Designate a DPO and ensure he/she has access to top management. This can be done either through direct reporting on the organizational structure, or through membership in the executive committee. It is important that your DPO is up-to-date on the strategic issues and change drivers that are impacting your organization.
- ☐ Send out an announcement to the organization that the DPO is the "privacy champion" and the point of contact within the organization for anything related to compliance with the Data Privacy Act.
- ☐ Make compliance to the Data Privacy Act part of the performance bonus criteria of divisions of the organization who are involved with privacy compliance, such as HR, Legal, IT, Security, etc.
- ☐ If your organization is considered medium- or high-risk in terms of privacy impact, consider forming a data protection task force or committee, and keep in mind that an organization can have more than one DPO. This allows DPO skills, expertise and tasks to be distributed across the entire DPO team. However, it should be clear who holds overall responsibility and accountability.
- ☐ Assign the head of Legal to ensure that all service provider contracts, job orders, etc. are compliant. For example, all service providers must also have their own DPO.
- ☐ Assign the head of Legal to ensure that all external sharing of data meets the required guidelines of the NPC.

Within 90 days:

- ☐ Support your DPO in scheduling PIA workshops, and in ensuring that the process owner(s) take full ownership of the PIA outputs.
- ☐ Ask DPO for the calendar of training and education events related to privacy management.
- ☐ Drive the urgency within the organization to comply with the Data Privacy Act.
- ☐ Assign head of HR to issue security clearances to all organization personnel and consultants who process personal data.

Within 180 days:

- ☐ Ensure that breach drills are being conducted on a regular basis.
- ☐ Ask DPO for results of the IT Security audit and the Privacy Impact Assessments.

For questions or comments on this checklist, please contact info@privacy.gov.ph

NATIONAL PRIVACY COMMISSION