

## Data Privacy Act (RA 10173) Checklist

### Signs of Compliance, Commitment to Comply, Capacity to Comply vs. Signs of Negligence

#### Pillar 1: Commit to Comply: Appoint a Data Protection Officer (DPO)

##### Sec. 21 of the DPA, Section 50 of the 50, Circular 16-01, and Advisory 17-01

<b>Appoint an individual accountable for compliance</b>	<b>Ineffective data protection governance</b>
<ul style="list-style-type: none"><li><input type="checkbox"/> Notarized designation of a DPO/COP, filed with the NPC</li><li><input type="checkbox"/> Evidence that DPO/COP recommendations are taken into consideration when making decisions</li><li><input type="checkbox"/> Contact details are easy to find (e.g. on website)</li><li><input type="checkbox"/> Continuing education program for the DPO/COP</li></ul>	<ul style="list-style-type: none"><li><input type="checkbox"/> No DPO or COP (in which case CEO or HoA is the default DPO)</li><li><input type="checkbox"/> Lack of interaction between DPO/COP and top management</li><li><input type="checkbox"/> Lack of interaction between DPO/COP and functional units</li><li><input type="checkbox"/> Communication from the DPO/COP is largely ignored</li><li><input type="checkbox"/> No continuing education program for the DPO/COP</li></ul>

#### Pillar 2: Know Your Risks: Conduct a Privacy Impact Assessment (PIA)

##### Sec. 20(c) of the DPA, Section 29 of the IRR, Advisory 17-03

<b>Know the risks represented by the processing to the rights and freedoms of data subjects</b>	<b>Data processing controls do not take into account the risks to the rights and freedoms of data subjects</b>
<ul style="list-style-type: none"><li><input type="checkbox"/> Up-to-date organizational inventory of processes that handle personal data, including the list of process owners</li><li><input type="checkbox"/> PIAs have been conducted, and are owned and kept up-to-date by the process owner</li><li><input type="checkbox"/> Stakeholders (those involved in the information life cycle) have been consulted as part of the PIA process</li><li><input type="checkbox"/> PIA includes a privacy risk map, a list of controls, an implementation plan, and a monitoring/evaluation milestone</li></ul>	<ul style="list-style-type: none"><li><input type="checkbox"/> No PIAs</li><li><input type="checkbox"/> Process owners do not “own” the PIAs</li><li><input type="checkbox"/> PIAs are not updated when changes are made to the process or to the technologies being used in the process\</li><li><input type="checkbox"/> Stakeholders are not consulted for the PIA</li><li><input type="checkbox"/> Controls identified during the PIA are not implemented</li></ul>

#### Pillar 3: Write Your Plan: Create Your Privacy Management Program (PMP)

##### Sec. 11-15 of the DPA, Sections 21-23 and 43-45 of the IRR, Circulars 16-01 and 16-02

<b>Processing of data is according to privacy principles of transparency, legitimate purpose, and proportionality</b>	<b>Data processing not according to privacy principles of transparency, legitimate purpose, and proportionality</b>
<ul style="list-style-type: none"><li><input type="checkbox"/> Personal data is processed as per Sections 12 and 13 of the DPA</li><li><input type="checkbox"/> Privacy principles are embedded into HR, Marketing, Operations, Security, and IT policies, are cascaded throughout the organization, and are updated as needed</li><li><input type="checkbox"/> Data handlers have security clearance and privacy training</li><li><input type="checkbox"/> Privacy notices are posted where appropriate (e.g. on website)</li><li><input type="checkbox"/> Data sharing agreements are in place</li><li><input type="checkbox"/> Tools in place to monitor compliance of the organization</li><li><input type="checkbox"/> Records of data processing are maintained</li></ul>	<ul style="list-style-type: none"><li><input type="checkbox"/> Processing fails to meet the criteria for lawful processing of personal data</li><li><input type="checkbox"/> No privacy policy</li><li><input type="checkbox"/> Privacy policy exists, but is not cascaded throughout the organization</li><li><input type="checkbox"/> No privacy training or security clearance for data handlers</li><li><input type="checkbox"/> Data is being shared without data sharing agreements</li><li><input type="checkbox"/> No records of data processing</li></ul>

**Pillar 4: Be Accountable: Implement your Privacy and Data Protection (PDP) Measures**

**Sec. 16-18 and 38 of the DPA and Sections 17-24, 34-37 of the IRR and Circular 16-04**

<b>Upholding the rights of data subjects</b>	<b>Neglecting the rights of data subjects</b>
<ul style="list-style-type: none"> <li><input type="checkbox"/> Data subjects are apprised of their rights through a privacy notice</li> <li><input type="checkbox"/> Consent is obtained prior to the collection and processing of data</li> <li><input type="checkbox"/> Data subjects are provided a means to access their data</li> <li><input type="checkbox"/> Data subjects are provided a venue to correct/rectify their data</li> <li><input type="checkbox"/> Data subjects know who to complain to if their rights are violated</li> <li><input type="checkbox"/> Complaints are acted upon quickly (within 30 days)</li> <li><input type="checkbox"/> These rights are upheld when invoked by the lawful heirs or assigns of the data subject</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> No privacy notice when collecting personal data</li> <li><input type="checkbox"/> Consent is not obtained prior to the collection/processing of data</li> <li><input type="checkbox"/> No venue for data subjects to access their data</li> <li><input type="checkbox"/> No venue for data subjects to correct/rectify their data</li> <li><input type="checkbox"/> No contact details on how to lodge a complaint</li> <li><input type="checkbox"/> Complaints take a long time to be remedied</li> <li><input type="checkbox"/> Inaction on complaints from data subjects</li> <li><input type="checkbox"/> Overcollection of personal data</li> </ul>

**Sec. 20.a-e, 22 and 24 of the DPA, Sections 25-29 of the IRR, Circular 16-01**

<b>Maintaining confidentiality, integrity, and availability</b>	<b>Insufficient controls to maintain confidentiality, integrity, and availability</b>
<ul style="list-style-type: none"> <li><input type="checkbox"/> Data protection risks have been identified and documented</li> <li><input type="checkbox"/> Appropriate and up-to-date organizational, physical, and technical controls are in place to manage these risks (e.g ISO:IEC 27002)</li> <li><input type="checkbox"/> Data protection policies are cascaded throughout the organization and updated as needed</li> <li><input type="checkbox"/> Vulnerability scanning is conducted at least once a year</li> <li><input type="checkbox"/> Business continuity drills are conducted at least once a year</li> <li><input type="checkbox"/> For data stored outside the Philippines, location of foreign country is defined</li> <li><input type="checkbox"/> For personal data stored in the cloud, NPC recommends that provider is ISO:IEC 27018 compliant (from Circular 16-01)</li> <li><input type="checkbox"/> For digitized personal data, NPC recommends 256-bit AES for data at rest and in transit (from Circular 16-01)</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Controls for data protection are not appropriate for the risks identified</li> <li><input type="checkbox"/> Controls for data protection are not updated for new risks/threats</li> <li><input type="checkbox"/> Controls for data protection are not complied with</li> <li><input type="checkbox"/> Cyber-hygiene practices are lax</li> <li><input type="checkbox"/> Business continuity drill has not been conducted in the last 12 months</li> <li><input type="checkbox"/> Security vulnerability scanning has not been conducted in the last 12 months</li> </ul>

**Pillar 5: Be Prepared: Regularly exercise your Breach Reporting Procedures (BRP)**

**Sec. 20.f and 30 of the DPA, Sections 38-42 and 57 of the IRR, Circular 16-03**

<b>Able to report breach within 72 hours</b>	<b>Unable/unwilling to report breach within 72 hours</b>
<ul style="list-style-type: none"> <li><input type="checkbox"/> Formation of a data breach response team with clearly defined roles and responsibilities</li> <li><input type="checkbox"/> Clearly defined and up-to-date incident response procedure</li> <li><input type="checkbox"/> Breach drills are conducted at least once a year</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> No breach response team</li> <li><input type="checkbox"/> No breach response policy or procedures</li> <li><input type="checkbox"/> Breach drill has not been conducted in the last 12 months</li> <li><input type="checkbox"/> No notification of the NPC within 72 hours of discovery of a breach of personal data (possible criminal offense)</li> </ul>

**Pillar 6: Registration**

**Sec. 24 of the DPA, and Sections 33 and 46-49 of the IRR, Circular 17-01**

<b>Register with the NPC</b>	<b>Non-registration with the NPC</b>
<ul style="list-style-type: none"><li><input type="checkbox"/> Registration with the NPC is up-to-date and contains all necessary compliance documentation</li><li><input type="checkbox"/> Registration of all automated processing operations that have legal effect on the data subject</li><li><input type="checkbox"/> Annual report summarizing documented security incidents and personal data breaches</li><li><input type="checkbox"/> Service providers are also registered</li></ul>	<ul style="list-style-type: none"><li><input type="checkbox"/> No registration (must be renewed annually)</li><li><input type="checkbox"/> Out-of-date registration (must be updated within three months of any change)</li><li><input type="checkbox"/> Non-reporting to NPC of documented security incidents and personal data breaches</li></ul>

**Sec. 14 of the DPA, Sections 43-45 of the IRR, Circular 17-01**

<b>Service providers agree to honor their compliance obligations</b>	<b>Service providers in default of their compliance obligations</b>
<ul style="list-style-type: none"><li><input type="checkbox"/> All service providers are contractually bound to comply with the DPA, the IRR, and NPC issuances</li></ul>	<ul style="list-style-type: none"><li><input type="checkbox"/> Service providers are not honoring their compliance obligations (includes registering with the NPC)</li></ul>

For questions or comments on this checklist, please contact [info@privacy.gov.ph](mailto:info@privacy.gov.ph) (Version: 24 July 2017)