Data Protection Compliance Plan Checklist

Personal Data Protection Law ("PDPL") No 151 of 2020

Table of Contents

I. PDPL Material & Territorial Scope

PDPL Material Scope				
	Yes	**No**	**Partial**	**NA**
1. Is personal data processed through fully or partially automated means (e.g., using electronic systems for collection, storage, use, or transfer)?				
2. Is any personal data maintained solely in manual or paper-based formats, without being subject to any electronic or automated processing? ***Note*:** If the answer to the question is "Yes" and there is no associated electronic processing, the PDPL does not apply to this data.				
PDPL Territorial Scope				
	Yes	**No**	**Partial**	**NA**
3. Are you an Egyptian controller or processor established or operating inside Egypt?				
4. Are you an Egyptian controller or processor established or operating outside Egypt?				
5. Are you a foreign controller or processor located within the Arab Republic of Egypt? (Regardless of the data subject's nationality or residence)				
6. Do you process personal data of Egyptian citizens residing inside or outside Egypt?				
7. Do you process personal data of foreign nationals residing within the Arab Republic of Egypt?				

II. Data Protection Principles and Legal Basis Alignment under Art. 3 and Art. 6 of the PDPL

1. Lawfulness of Processing

	Yes	**No**	**Partial**	**NA**
8. Do you determine and document a valid lawful basis (e.g., consent, contract, legal obligation, legitimate interest) for each processing activity?				

- **If the consent is relied upon as the lawful basis:**

General Consent Requirements				
Consent must be **explicit**, **freely given**, **specific**, **informed**, and **unambiguous,** and obtained through **a clear affirmative action**.	**Yes**	**No**	**Partial**	**NA**
a. Is the consent explicit, freely given, specific to a declared and legitimate purpose, informed, and unambiguous?				
b. Is the consent request presented clearly and separately from general terms and conditions, in plain, intelligible, and accessible language? (**consent is not bundled with other terms and conditions)**				
c. Do individuals need to take a positive action to indicate their agreement (i.e., opt-in)?				
d. Are separate consents obtained for distinct processing activities or purposes, with each request clearly explaining the type of processing and its corresponding purpose?				
e. Are individuals clearly informed of their right to refuse or withdraw consent at any time, without detriment?				
f. Are effective, simple mechanisms provided for individuals to withdraw consent at any time?				
g. Are individuals able to continue receiving the service even if they decline to provide consent for optional processing? (i.e., consent is not a condition of service)				
h. Are records of consent obtained documented and securely maintained?				
i. Are consent practices regularly reviewed and updated? Note: C**onsent Practices** refers to the **set of policies, procedures, and operational measures** an organization puts in place to **obtain, manage, and demonstrate valid consent** from data subjects.				
Consent for Sensitive Personal Data				
Where the processing concerns **sensitive personal data**, **additional conditions must be assessed**	**Yes**	**No**	**Partial**	**NA**
a. Is the consent **explicit**, **written**, and obtained directly from the data subject or their authorized representative? (Consent may be obtained in physical or electronic format.)				
Consent for Children's Data				
Additional safeguards apply when processing data of **children under 18. The following conditions must be assessed**	**Yes**	**No**	**Partial**	**NA**

a. **For children under the age of 15:** - Is **explicit consent** obtained from the parent or legal guardian specifying the purpose and duration of the processing? b. **For children aged 15 to 18:** - Has the child (or their guardian, as applicable) submitted the guardian's **explicit consent** for collection and processing?				

- **If the contractual obligation is relied upon as the lawful basis:**

	Yes	No	Partial	NA
a. Is there a contract or pre-contractual obligation with the data subject?				
b. Is the processing necessary to perform the contract or enter into a contract?				
c. Is the processing limited to what is strictly required to fulfill the contract or pre-contractual obligation?				

- **If the legal obligation is relied upon as the lawful basis:**

	Yes	No	Partial	NA
a. Is the processing necessary to comply with a specific legal obligation imposed by applicable legislation?				
b. Has the relevant legal provision or regulatory requirement been clearly identified and documented?				
c. Is the processing proportionate and limited to what is required to fulfil the identified legal obligation?				

- **If the legitimate interest is relied upon as the lawful basis:**

	Yes	No	Partial	NA
a. Has a specific and legitimate interest been clearly identified and documented for the processing activity?				
b. Is the processing necessary to achieve that interest, and is there no less intrusive, reasonable alternative?				
c. Would the data subject reasonably expect this processing, given the nature of the relationship and context?				
d. Can the processing be stopped if the data subject objects, unless compelling legitimate grounds are demonstrated?				

e. Can you demonstrate accountability for this legal basis through internal documentation and review procedures?				

2. Fairness

	Yes	No	Partial	NA
a. Have you evaluated whether your data processing could lead to any unjustified harm to individuals?				
b. Are individuals' expectations taken into account when collecting and using their data?				
c. Have you conducted risk assessments for any high-impact processing that could negatively affect data subjects?				

3. Transparency

Transparency Information				
	Yes	**No**	**Partial**	**NA**
a. Have you ensured that all required information relating to the purposes, legal basis, and methods of personal data processing is provided to data subjects in a clear, concise, and intelligible format?				
b. Is the transparency information provided to data subjects prior to or at the time of personal data collection?				
c. Is the transparency information made easily accessible through appropriate communication channels (e.g., website, mobile application, or physical form)?				
d. Do you clearly inform data subjects of their **rights** (e.g., right of access, correction, erasure, objection, and withdrawal of consent)?				
Accessibility and Maintenance of Privacy Notices &Privacy Policies				
	Yes	**No**	**Partial**	**NA**
a. Do you **maintain a public-facing privacy notice** that clearly outlines the purposes, lawful basis, and methods of all personal data processing activities?				
b. Is your privacy notice or equivalent communication **periodically reviewed**, kept up to date, and revised?				

c. Do you have an **internal privacy policy** that instructs employees on lawful, secure, and transparent handling of personal data?				
Compelled Disclosure				
	Yes	**No**	**Partial**	**NA**
a. Do you have an internal policy governing compelled disclosures to law enforcement or regulatory authorities, ensuring legal validity and proper documentation? Note: **Compelled disclosure** means the obligation to disclose or hand over personal data (or other types of information) because of a **legal or regulatory requirement**.				

4. Purpose Limitation

	Yes	**No**	**Partial**	**NA**
a. Are processing purposes clearly defined and specific prior to data collection?				
b. Do you ensure data is not further processed in ways incompatible with the original purposes?				
c. Are secondary uses of personal data assessed for compatibility or supported by a new legal basis?				

5. Data Minimization

	Yes	**No**	**Partial**	**NA**
a. Have you ensured that only personal data which is adequate, relevant, and strictly necessary for the specified and legitimate purpose is collected and processed?				
b. Have all data collection mechanisms (including forms, systems, and datasets) been reviewed to identify and eliminate unnecessary or excessive data fields?				

6. Storage Limitation

	Yes	**No**	**Partial**	**NA**
a. Have clearly defined and documented data retention periods been established for each processing activity?				

b. Are these retention periods consistent with the lawful purpose of collection and any applicable legal obligations?				
c. Are appropriate procedures in place to ensure that personal data is securely deleted or anonymized upon the expiration of the applicable retention period?				
d. Are periodic reviews conducted to identify and remove personal data that is no longer necessary?				

7. Data Accuracy

	Yes	No	Partial	NA
a. Are appropriate measures in place to ensure that personal data is accurate and, where necessary, kept up to date, including through periodic verification and rectification mechanisms?				
b. Does the controller provide accessible and effective means for data subjects to request the correction or update of inaccurate or incomplete personal data?				

8. Data Security

Preliminary Assessment				
	Yes	**No**	**Partial**	**NA**
a. Have appropriate technical measures (such as encryption, access controls, and intrusion detection systems) been implemented to ensure the confidentiality, integrity, and availability of personal data?				
b. Are there documented organizational measures (including internal policies, employee training, breach response protocols, and third-party oversight) in place to support secure and lawful processing?				
Governance and Accountability				
	Yes	**No**	**Partial**	**NA**
a. Is there a documented governance framework for managing information security, privacy risks, and compliance?				
b. Are roles, responsibilities, and accountabilities clearly defined and regularly updated at all levels?				

c. Is there a steering committee or oversight body overseeing the alignment of information security and privacy with strategic objectives?				
d. Are adequate resources and skills allocated for effective privacy and information security management?				
e. Is segregation of duties implemented and reviewed to reduce unauthorized actions?				
f. Is there a privacy risk management process to assess, treat, monitor, and communicate personal data risks?				
g. Are privacy risk management processes established?				
Privacy by Design and by Default				
	Yes	**No**	**Partial**	**NA**
a. Do you ensure that data protection is integrated into the design of your processing activities and business practices from the start?				
b. Is data protection, through both privacy impact considerations and technical safeguards, embedded into the design and development of systems, products, and services from the outset?				
c. Are there procedures in place to ensure personal data is automatically protected by default and is not made accessible to an indefinite number of persons?				
d. Do you have procedures in place to ensure that personal data is automatically protected in any IT system or business practice?				
e. Do you ensure that privacy settings are set to the most privacy-friendly options by default?				
f. Do you conduct Data Assessments? (Data Protection Impact Assessment (DPIA), Risk Assessment, Vendor Assessment …etc.)				
Technical and Organizational Security Measures				
	Yes	**No**	**Partial**	**NA**
a. Are encryption mechanisms enforced to maintain personal data confidentiality and integrity?				
b. Do you use pseudonymization where applicable to enhance data security?				
c. Are physical security controls in place to protect personal data confidentiality, integrity, and availability?				
d. Do you apply secure configuration and vulnerability management practices for systems processing personal data?				
e. Are secure procedures documented and followed for disposing of personal data media?				
f. Are secure communication safeguards in place for internal and external personal data transmission?				

Monitoring, Audit, and Risk Mitigation				
	Yes	**No**	**Partial**	**NA**
a. Are continuous monitoring mechanisms, regular audits, and assessments in place?				
b. Are policy reviews and updates implemented with metrics and analysis tools?				
c. Is there an asset management process for assets associated with personal data?				
d. Are access control safeguards implemented for personal data-related assets?				
e. Are there documented procedures for secure personal data management?				
Training & Awareness				
	Yes	**No**	**Partial**	**NA**
a. Do you have any privacy awareness programs that are adopted?				
b. Do you provide training and awareness programs for employees to understand and implement privacy by design and by default principles?				
Certifications and External Standards				
a. Can you list the certifications your organization complies with related to information security and privacy? 1) ……. 2) ……. 3) ……. 4) …….				

9. Accountability

The following condition must be assessed	Yes	No	Partial	NA
a. Can the controller demonstrate full compliance with the data protection principles through verifiable documentation, such as Records of Processing Activities ("ROPA"), Data Protection Impact Assessments ("DPIAs"), internal policies, audit logs, consent logs, and training records?				

a. Record of Processing Activities ("ROPA")

Important Note:

- Article 4-9 mandates that **controllers** maintain a **Record of Processing Activities ("ROPA")**.

- Article 5-9 requires the same for **processors**, for the processing activities they perform on behalf of controllers.

Data Inventory				
	Yes	**No**	**Partial**	**NA**
a. Do you define personal and sensitive personal data in accordance with Article 1 of the PDPL? [*You clearly understand and apply the legal definition of personal and sensitive personal data under the PDPL to ensure accurate identification and classification.]*				
b. Do you identify all personal information collected and used by the organization? [*You determine what personal data is collected, the purposes, the means of collection, and how it is used across your operations.]*				
c. Do you document where personal information is stored? [*You record all storage locations, including internal systems, third-party platforms, geographic server locations, and data centers.*]				
d. Do you map the flow of personal information across your organization? [*You visualize the lifecycle of personal data—from collection through processing, storage, and transmission—including data sharing with vendors or third parties.]*				
e. Do you determine and document the retention periods for personal data?				
f. Do you classify and categorize personal data? [*You assign appropriate classification levels (e.g., public, confidential, restricted) and evaluate the risk level associated with each category of personal data.*]				
g. Do you document the authority and responsibility for systems processing personal data? [*You record the individuals or departments responsible for the systems that handle personal data, including their roles and decision-making authority.*]				
Record of Processing Activities ("ROPA") – Controller Requirements (Article 4-9)				
If you are a controller, does your documentation include the following?	**Yes**	**No**	**Partial**	**NA**
a. Name and contact details of the controller				
b. Name and contact details of the controller's representative (if applicable)				

c. Name and contact details of the Data Protection Officer ("DPO")				
d. Name and contact details of any joint controller (if applicable)				
e. Purpose(s) of personal data processing				
f. Record of consent				
g. Description of the categories of personal data processed				
h. Description of the categories of data subjects [In practical terms, it means: You must describe the types of people whose personal data you collect, store, use, or transfer.]				
i. Description of the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organizations				
j. Access control mechanisms				
k. Procedures for erasure or modification of personal data				
l. Identification of any third countries or international organizations to which personal data is transferred & Documentation of appropriate safeguards for international data transfers				
m. Retention periods for each data category				
n. General description of technical and organizational security measures				
o. Description of data subject rights available under the PDPL				
Record of Processing Activities ("ROPA") – Processor Requirements (Article 5-9)				
If you are a processor, does your documentation include the following?	**Yes**	**No**	**Partial**	**NA**
a. Name and contact details of the processor or processors and each controller on behalf of which the processor is acting				
b. Name and contact details of the controller's representative or the processor's representative (if applicable)				
c. Name and contact details of the Data Protection Officer ("DPO")				
d. Categories of processing activities carried out on behalf of each controller				
e. Procedures for erasure or modification of personal data				
f. Retention periods for each data category				
g. Identification of any third countries or international organizations to which personal data is transferred & Documentation of appropriate safeguards for international data transfers				

h. General description of technical and organizational security measures				

III. Responding to Data Subject Requests

Data Subject Rights Enablement				
	Yes	**No**	**Partial**	**NA**
a. Do you have a documented and operational process to enable data subjects to exercise their rights under the PDPL, such as mechanisms for submission, identity verification, and response handling?				
b. Do your procedures ensure that acknowledgement of data subject requests is issued within six working days, as legally required?				
c. Are responses to data subject requests provided in a clear, intelligible, and accessible format using plain language?				
Rights Covered by Internal Procedures				
Confirm that internal procedures adequately cover the following rights	**Yes**	**No**	**Partial**	**NA**
Right to be informed				
Right of access				
Right to withdraw consent				
Right to erasure				
Right to restrict processing				
Right to data portability				
Right to object				
Right to rectification				
Right to be notified in case of a data breach				

IV. Data Protection Officer

Appointment & Nationality of DPO				
	Yes	**No**	**Partial**	**NA**
a. Is a Data Protection Officer (DPO) appointed for the organization?				

Is the DPO: ☐ Egyptian ☐ Foreign National				
Employment Status of DPO				
	Yes	**No**	**Partial**	**NA**
a. Is the DPO an existing employee of the organization? **Disclaimer:** The DPO may be an existing employee of the organization and may retain their previous responsibilities, provided that the conditions of independence are upheld and the role has been approved by PDPC has approved the role during the registration process.				
b. Does the DPO continue to perform previous job functions alongside the DPO role?				
c. Is the DPO involved in decision-making regarding personal data processing activities?				
d. Is the DPO a newly hired employee or externally contracted? ☐ New hire ☐ External consultant/service provider				
e. <u>External DPO Appointments: (If applicable)</u> 1. If the same DPO is appointed to serve multiple controllers or processors, has prior approval been obtained? 2. In the case of a shared DPO arrangement across more than one entity, have all involved controllers or processors formally provided their written consent to such arrangement?				
DPO Roles and Responsibilities Based on Article 9 of Law No. 151 of 2020				
<u>Monitoring and Evaluation</u>	**Yes**	**No**	**Partial**	**NA**
a. Does the DPO oversee and ensure the entity's compliance with the PDPL?				
b. Does the DPO monitor and evaluate the performance of departments involved in data processing activities?				
c. Does the DPO review the organizational (e.g., policies, procedures) and technical controls implemented to ensure compliance with the PDPL?				
d. Does the DPO determine the scope and frequency of compliance assessments? [*Focus:* Legal and procedural obligations under the PDPL.]				
e. Does the DPO ensure that appropriate data assessments, such as Data Protection Impact Assessments ("DPIAs"), Transfer Impact Assessments ("TIAs"), or similar evaluations, are carried out to identify and mitigate risks related to personal data processing activities?				

f. Does the DPO ensure that assessments are carried out by appropriate personnel or third-party experts?				
g. Does the DPO review findings and recommendations from compliance assessments and data assessments?				
h. Does the DPO report on the entity's overall data protection compliance status to management?				
Enabling Data Subject Rights	**Yes**	**No**	**Partial**	**NA**
a. Does the DPO ensure that data subjects can effectively exercise their rights under the PDPL, including the handling of their requests and complaints in a timely and transparent manner?				
b. Is the DPO's contact information made available and easily accessible to data subjects?				
Incident Management	**Yes**	**No**	**Partial**	**NA**
a. Does the DPO notify the data subjects in the event of a personal data breach or violation?				
b. Does the DPO ensure that corrective measures are taken to address and contain personal data breaches and to eliminate violations related to personal data?				
Record Keeping and Maintenance	**Yes**	**No**	**Partial**	**NA**
a. Does the DPO oversee the maintenance and updating of the record of processing activities (ROPA) held by the controller, and the relevant processing operations record held by the processor, while ensuring the accuracy and completeness of the recorded data?				
Training and Capacity Building	**Yes**	**No**	**Partial**	**NA**
a. Does the DPO organize training programs for employees to ensure their compliance with the PDPL?				
Position and Independence				
The following condition must be assessed	**Yes**	**No**	**Partial**	**NA**
a. Is the DPO positioned at a sufficiently senior level within the organizational structure?				
b. Is the DPO assigned a position that ensures independence in the performance of their duties?				
c. Is the DPO guaranteed protection against dismissal or disciplinary action for performing their duties in compliance with the PDPL?				
d. Does the DPO report directly to the highest level of management (e.g., CEO, Board of Directors)?				
Certifications				
Does your Data Protection Officer (DPO) hold professional certifications such as CIPP/E, CIPM, or CIPT? If yes, please list the certifications 1) …….. 2) …….. 3) ……..				

4) ……..

V. Licenses and Permits Readiness

Controller / Processor - Processor		
	Yes	**No**
a. Has your organization identified whether it qualifies as a Controller/Processor, or Processor for purposes of determining the applicable licensing or permit obligations?		
b. Are you aware that obtaining a license or a permit from the PDPC is required before processing personal data under the PDPL? **Note:** 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;		
c. Has your organization prepared the necessary documentation (e.g., data inventory, security measures, DPO designation) to support a license or permit application?		
Cross-Border Data Flow		
	Yes	**No**
a. Are you aware that a license or permit must be obtained from PDPC prior to conducting international data transfers under the PDPL, once such procedures are formally issued?		
b. Have you assessed your current data flows in preparation for these future licensing requirements?		
Electronic Marketing		
	Yes	**No**
a. Are you aware that conducting electronic marketing activities is subject to obtaining a license or permit from PDPC?		
b. Have you assessed your current and planned electronic marketing practices in preparation for future licensing or permit obligations under the PDPL?		
c. Do you regularly review and update your e-marketing practices to ensure compliance with the PDPL?		
Visual Surveillance Tools in Public Places		
	Yes	**No**
c. Are you aware that the installation and operation of visual surveillance tools in public places is subject to obtaining a license or permit from PDPC?		

d. Has your organization secured all necessary approvals from the competent authorities for the lawful use of visual surveillance tools in public places?		

VI. Cross-Border Data Transfer – Readiness Compliance Assessment

The following condition must be assessed	Yes	No	Partial	NA
a. Do you currently process personal data outside the territory of the Arab Republic of Egypt?				
b. If yes, have you identified the transfer basis on which each external data transfer is carried out?				
c. Have you documented all relevant jurisdictions and their current adequacy status in anticipation of future PDPC determinations?				
d. In the absence of any adequacy decision, have you implemented appropriate safeguards to justify the transfer in accordance with the PDPL and its Executive Regulation?				
e. Are mechanisms in place to ensure that the data importer applies protection measures equivalent to those under the PDPL?				
f. If neither adequacy nor safeguards apply, have you assessed whether your transfers qualify for one of the limited derogatory cases permitted under the PDPL?				
g. If relying on exceptional transfer cases (derogations), have you documented the basis for each transfer?				
h. Have you carried out and documented a transfer impact assessment (TIA) to evaluate legal and technical risks associated with cross-border transfers?				

VII. Electronic Direct Marketing

Consent and Record-Keeping				
	Yes	No	Partial	NA
a. Do you obtain and verify the consent of the Data Subject before sending any electronic communication for direct marketing?				
b. Do you ensure that direct marketing communications are sent only to Data Subjects who have explicitly opted in?				
c. Do you maintain electronic records evidencing the Data Subject's consent or non-objection to receive e-marketing				

communications, including any amendments, for a period of three years from the date of the last communication?				
Transparency and Communication Content				
	Yes	**No**	**Partial**	**NA**
a. Does each electronic marketing communication clearly identify the sender and creator, include a valid contact address, and indicate its purpose as direct marketing?				
b. Do you specify a defined marketing objective for each electronic marketing communication sent to Data Subjects?				
Data Subject Rights and Preferences				
	Yes	**No**	**Partial**	**NA**
a. Do you ensure that the Data Subject is presented, from the outset, with a clear and unambiguous option to decline consent to receive electronic marketing communications?				
b. Do you ensure that the Data Subject is not compelled to consent to receiving electronic marketing communications as a condition for accessing a service, unless such communication is objectively necessary for the performance or provision of that service?				
c. Do you ensure that the Data Subject can withdraw previously granted consent or opt out of receiving further electronic marketing communications at any time through a clear and easily accessible mechanism?				
d. Do you offer a simple and easily accessible process through which Data Subjects can modify, update, or manage their communication preferences (e.g., frequency, channel, or type of marketing content)?				
e. Do you ensure that the contact details of the Data Subject are not disclosed in your e-marketing communications?				

VIII. Visual Surveillance Tools in Public Places

	Yes	**No**	**Partial**	**NA**
a. Has your organization placed clear and visible privacy notices in public areas to inform individuals of the presence and operation of visual surveillance tools				
b. Has your organization ensured that any recordings or images obtained through visual surveillance tools are not transferred, made available, or processed outside the territory of the Arab Republic of Egypt, except where expressly permitted by law?				
c. Has your organization ensured that no processing is carried out on personal images or video recordings using facial				

recognition or similar identification technologies, except where expressly permitted by law or based on the explicit consent of the data subject?				
d. Has your organization implemented binding measures to ensure that personnel operating visual surveillance systems in public places are obligated to maintain the confidentiality of collected data and are prohibited from using, sharing, or disclosing such data except as expressly permitted by law?				
e. Has your organization implemented the technical and organizational measures to secure recordings obtained through visual surveillance systems and to protect them against unauthorized access, breaches, or misuse?				

IX. Vendor and Third-Party Risk Management

	Yes	No	Partial	NA
a. Policies and Procedures Are vendor assessment policies consistently followed by all departments?				
b. Ongoing Monitoring and Auditing Is there regular monitoring and auditing of vendor activities?				
c. Termination Process Is there a clear process for terminating the vendor relationship?				
d. Data Inventory/Map Is relevant personal information included in your data inventory/map?				
e. Procurement Process Is there a consistent procurement process in place?				
f. Contractual Requirements Are all privacy and security requirements addressed in the contract?				
g. Processing Activities Do processing activities align with the privacy framework?				
Privacy Risk Management a. Is a vendor/third-party risk assessment conducted prior to engagement?				
b. Are compliance certifications, privacy policies, and information security policies reviewed before finalizing agreements?				

c. Are privacy risks identified, assessed, mitigated, and addressed in the contract?				
a. <u>Training and Awareness</u> Have relevant teams received training to handle vendor privacy issues?				

X. Data Breach Response Plan Compliance

<u>Breach[1] Notification Obligations</u>				
Internal Preparedness and Existing Procedures	**Yes**	**No**	**Partial**	**NA**
a. Has your organization adopted an incident response plan addressing personal data breach?				
b. Does the incident response plan clearly identify all required notification recipients, including affected data subjects and, in the case of processors, the controller or other relevant parties?				
c. Does the incident response plan establish procedures and timelines triggered upon becoming aware of a personal data breach?				
Anticipated Obligations upon Official Launch of PDPC	**Yes**	**No**	**Partial**	**NA**
Has your organization reviewed and accounted for future breach notification obligations in its documented incident response plan, specifically with respect to procedures that: a. Provide for notifying the Personal Data Protection Center (PDPC) within seventy-two (72) hours of becoming aware of a personal data breach?				
b. Provide for notifying the PDPC immediately in cases involving breaches that impact national security?				
c. Provide for notifying affected data subjects within three (3) working days of notifying the PDPC? *Note:* This focuses on the **present state of documentation**: whether the current plan already reflects the statutory obligations (even if not yet enforceable).				
d. If the above is not implemented, is your organization currently preparing specific updates to your breach response framework to operationalize the statutory breach notification obligations under the PDPL? *Note*: This focuses on the **future implementation.**				
<u>Incident[2] Detection and Immediate Response</u>				

	Yes	No	Partial	NA
Are there procedures for: a. **Detecting personal data breaches** effectively?				
b. **Monitoring data security** to promptly identify incidents?				
c. **Taking immediate containment and remediation actions** once a breach is suspected or confirmed?				
Incident Response Plan Structure and Governance				
	Yes	**No**	**Partial**	**NA**
a. Does the incident response plan define internal escalation mechanisms and assign clear roles and responsibilities to relevant personnel, including the designation of an **Incident Response Team (IRT)** responsible for managing and responding to personal data breaches?				
b. Does the plan include structured procedures for? • **Containment, and recovery** • **Post-incident reviews** and implementation of **corrective actions**				
c. Is the incident response plan formally embedded within the organization's overarching risk management and data security governance frameworks, and does it undergo **periodic review and update to** maintain compliance with applicable legal obligations and ensure operational effectiveness?				
Communication and Training				
	Yes	**No**	**Partial**	**NA**
d. Are **training and awareness programs** in place to ensure that all employees are familiar with breach reporting procedures and the legal implications of data incidents?				
Documentation and Reporting				
	Yes	**No**	**Partial**	**NA**
Does the organization maintain complete documentation for each incident, including? a. **Incident description**				
b. **Response actions taken**				
c. **Lessons learned** and **post-incident remediation measures**?				
Annex: Key Definitions				

1. **Incident**: An event that may compromise the confidentiality, integrity, or availability of personal data, but which does **not necessarily trigger notification obligations**.

2. **Breach**: A **confirmed unauthorized disclosure** of personal data, which **requires notification** to external parties under the PDPL.

XI. Website/App-Specific Compliance

Controllers, and processors acting on their behalf, who operate websites or mobile applications must ensure full compliance with all provisions of the PDPL and its Executive Regulation. The checklist below outlines specific requirements applicable to personal data processing activities carried out through digital platforms. These obligations are **complementary** to, and must be implemented alongside, the other requirements addressed in other thematic compliance checklists

Privacy Interface and User Interaction				
	Yes	**No**	**Partial**	**NA**
a. Is a dedicated and up-to-date privacy notice made publicly available on the website/app, clearly describing the personal data collection and processing activities carried out through the digital platform?				
b. Is the Privacy Notice **easily accessible on every page** (e.g., via footer or menu)?				
Cookie and Tracking Consent (Digital Environment)				
	Yes	**No**	**Partial**	**NA**
a. Is a cookie banner implemented that clearly explains the use and purposes of cookies, pixels, SDKs, or similar tracking technologies, and distinguishes between essential and non-essential types?				
b. Are non-essential cookies and tracking technologies disabled by default and only activated after obtaining the user's explicit, informed consent?				
c. Does the consent interface provide **granular options** by category (e.g., performance, analytics, marketing), rather than relying solely on general acceptance or refusal, enabling users to select or refuse specific categories of cookies or similar technologies?				
d. Once preferences are submitted, are they **properly recorded and enforced across future sessions**, unless the Data Subject revokes or modifies them?				
e. Is a clearly accessible mechanism provided for users to review, modify, or withdraw their cookie preferences at any time?				

f. Does the website/app remain fully usable and accessible even when the user declines all non-essential cookies?				
g. Is the cookie banner linked to the Privacy Notice and accessible from all pages?				
Third Party and Data Processor Alignment				
	Yes	**No**	**Partial**	**NA**
a. Have you identified all **third parties or processors** involved in website/app operations (e.g., hosting, analytics, marketing tools)?				
Do all processor contracts include provisions that bind them to PDPL-compliant obligations?				
Have you reviewed whether each third party aligns with your published Privacy Notice?				
Are regular reviews conducted to ensure third parties remain compliant with PDPL?				
Website/Application Security Measures				
	Yes	**No**	**Partial**	**NA**
Have you implemented **technical and organizational measures** to secure personal data processed through your website or app?				
Are third-party scripts and plugins regularly reviewed for vulnerabilities?				
Do you have a digital-specific incident response procedure in place for handling personal data breaches involving the website/app, including secure user notification channels?				
Age Verification Measures				
	Yes	**No**	**Partial**	**NA**
If your website/app targets or may be used by children, do you implement **age verification mechanisms** and obtain **verifiable parental consent** before collecting personal data?				
Content Management System (CMS) and Plugin Updates				
	Yes	**No**	**Partial**	**NA**
Is your CMS regularly **updated and patched** to prevent vulnerabilities?				
Are third-party plugins or extensions kept up to date and legally reviewed?				
Data Subject Communication and Rights Requests				
	Yes	**No**	**Partial**	**NA**
Does the website/app provide a clearly visible and consistently accessible communication channel (e.g., privacy-specific email address, contact form, or in-app feature) through which Data Subjects may submit inquiries, complaints, or exercise their rights under the PDPL?				
Is there a documented internal procedure in place to: • Acknowledge receipt of Data Subject communications				

• Verify the identity of the requesting Data Subject prior to responding; • Record and log the nature of the request or complaint, the steps taken, the outcome, and the timeline of action taken				