SharkStriker

Bridging Cybersecurity & Compliance Gaps

PDPL Compliance Checklist For SMEs

01. Scope and Applicability

- [ ] Does it apply to you?
  - [ ] Yes (if you check any one or both, follow the checklist)
    - Do you process personal data within Saudi Arabia?
      or/and
    - Do you process personal data of individuals residing in Saudi Arabia?
  - [ ] No (PDPL does not apply to you.)

02. Register with SDAIA Data Governance Platform

- Data controllers may be required to register on the SDAIA National Data Governance Platform.
  - [ ] Determine if registration applies to you.
  - [ ] Register processing activities.
  - [ ] Maintain up-to-date information.

03. Governance

- [ ] Do you require a Data Protection Officer (DPO)?
- Assess whether a Data Protection Officer is required as per PDPL and appoint one if necessary.
  - [ ] Yes, if you:
    - Process large-scale personal data
    - Process sensitive data
    - Engage in high-risk activities
    - Are a public entity
  - [ ] No
- [ ] Appoint a Data Protection Officer (DPO)
- This is someone who can oversee the data protection activities overall and act as a contact point.
  - [ ] Have you designated an employee or hired a part-time consultant?
  - [ ] Have you documented their responsibilities and contact details?

04. Data Mapping

- [ ] Map personal data flows.
- Carry out an assessment to know what personal data you collect, why it is collected, where it's stored, with whom it is shared, and the retention periods.
  - [ ] Create a register with:
    - Data categories (like Names, Emails, IDs, and numbers).
    - Purpose of personal data collection.
    - Source.
    - Storage location of personal data (cloud/server etc.).
    - Any third party recipients.
    - Retention period.

05. RoPA

- [ ] Keep records of processing activities (RoPA).
- Document all of your processing related activities as per PDPL so you can demonstrate compliance.
  - [ ] Create a RoPA with:
    - Purposes
    - Data categories
    - Recipients
    - Transfers
    - Retention
    - Security measures
  - [ ] Update it annually or when processes change

06. Legal Basis

- [ ] Define lawful grounds and purpose limits.
  - Set lawful grounds and clear & specific purpose for each data processing activity. Data must never be used beyond the set purpose.
    - [ ] Create a section in register for:
      - Define legal basis (like consent, contractual necessity, legal obligation, legitimate purpose when permitted)
      - Explicit purposes.
- [ ] Accurately obtain and manage consent.
  - All consent must be informed, specific, given freely, and documented when required. This stands strongly especially for marketing or sensitive data.
    - [ ] Use clear consent statements.
    - [ ] Log consents with data and purpose.
    - [ ] Provide mechanism for easy opt-out.
    - [ ] Keep consent records for audit.

07. Transparency

- [ ] Create transparent privacy notices.
  - Tell people what data you are collecting of them, why, for how long you are going to keep it, and their rights.
    - [ ] Create and publish privacy notice on your website (in plain language). It should consist:
      - Data controller's identity.
      - Contact.
      - Purpose.
      - Lawful bases.
      - Retention.
      - Sharing details.
      - Rights.
      - DPO Details (if applicable).
    - [ ] Include privacy notice in employee onboarding and customer forms.

08. Data Subject Rights

- [ ] Implement data subject rights processes.
- Provide people a means to request access, correction, deletion, objection, or restriction, withdrawal of their personal data.
  - [ ] Create a simple procedure and templates to receive requests within PDPL time frames (document with time frame and procedure).
  - [ ] Verify identity of requesters before fulfilling requests.
  - [ ] Allow individuals to withdraw their consent at any time.
  - [ ] Provide a copy of their personal data upon request.

09. Security Controls

- [ ] Secure personal dat.
- Implement appropriate security measures to protect data from unauthorized access, loss or breach.
  - [ ] Implement hygiene measures (at minimum):
    - Use strong passwords.
    - Enable Multi-Factor Authentication for all the critical accounts.
    - Encrypt data at rest and in transit.
    - Keep systems and software updated.
    - Limit access on a need-to-know basis.
    - Take regular backups and test restores.
    - Keep an inventory of devices that store personal data.
  - [ ] Implement similar measures to protect deceased individuals' identity.

10. Vendors & Processors

- [ ] Manage third parties and processors.

- If you share data with vendors/processors, they must possess sufficient safeguards and act only on your instructions.
  - [ ] Prefer vendors who adhere with local and global compliance standards.
  - [ ] Create and maintain a vendor list.
  - [ ] Use written contracts that specify:
    - Processing purposes.
    - Security measures expected from vendors/processors.
    - Data breach notification duties.
    - Deletion/return of data.

11. Cross Border Transfers

- [ ] Handle cross-border data transfers accurately.

- Any transfer of data outside Saudi Arabia is only allowed if it does not harm national security and the organization has ensured adequate protections, used specific legal mechanisms, and taken SDAIA approval (if needed).
  - [ ] Assess legal basis of transfer.
  - [ ] Ensure adequate level of protection.
  - [ ] Implement contractual safeguards.
  - [ ] Obtain SDAIA approval (if required).
  - [ ] Create a section in your register that identifies transfers.
  - [ ] Set up mechanisms for transfer.
  - [ ] Use only approved transfer mechanisms (like contractual clauses and local requirements).
  - [ ] Minimize cross-border transfers.
  - [ ] Consult legal advice for any uncertain cases of transfer.

12. Data Lifecycle

- [ ] Maintain policies for data retention and deletion.

- Do not keep personal data beyond its purpose. Once the personal data doesn't serve the purpose, securely delete it and anonymize it.
  - [ ] Set retention periods for each data type in your register.
  - [ ] Implement routine deletion/archival processes.
  - [ ] Document secure data deletion processes.

13. Breach Management

- [ ] Prepare breach response plan and notification process.

- Have a mechanism to detect, contain, investigate, and report data breaches to authorities and affected people when required.
  - [ ] Create a simple incident response checklist (identify, contain assess, notify, remediate).
  - [ ] Define internal roles.
  - [ ] Create a mechanism to notify the competent authority, and data subjects without undue delay when if the breach is likely to cause harm to personal data or data subjects.
  - [ ] Create templates for communications.
  - [ ] Log all the incidents.

14. Risk Assessments & DPIA

- [ ] Conduct periodic risk assessments and DPIA.

- Assess the privacy risks associated with processing data and perform Data Protection Impact Assessments for high risk processes.
  - [ ] Review high risk activities regularly (like sensitive data processed on a large scale).
  - [ ] Use a simple template to record risks and mitigation steps.
  - [ ] For new projects perform DPIA with sensitive/extensive profiling.

15.Training & Awareness

- [ ] Train staff and enforce policies.
- Make employees aware of the privacy rules under PDPL and safe data handling best practices.
  - [ ] Provide privacy and security training annually and on employee onboarding
  - [ ] Create comprehensive and clear policies for:
    - Remote work.
    - Acceptable use.
    - Device security.
  - [ ] Require acknowledgement of the policies after creation and on every update.

16. Audits & Monitoring

- [ ] Use privacy by design and default.
- Incorporate privacy while creating new services and ensure that default settings are privacy protective.
  - [ ] Apply access controls and minimize data collection while launching new systems.
  - [ ] Document design decisions showing privacy measures.
- [ ] Maintain internal audit and review.
- Check whether your controls are working effectively and update controls based on regulatory/business changes.
  - [ ] Schedule an annual compliance review.
  - [ ] Record findings/ gaps identified.
  - [ ] Take corrective actions to bridge the compliance gaps.
- [ ] Ensure contracts and HR compliance.
- All the employment and service contracts should address data handling, confidentiality, and responsibilities of employees.
  - [ ] Add clauses for data protection in employment and vendor contracts.
  - [ ] Limit employee access to only necessary data.
- [ ] Prepare for regulator contact and requests.
- Be prepared for the competent authority's audit or requests for information about your processing.

- [ ] Maintain documentation of compliance (like RoPA, DPIAs, consents, data breach logs, and contracts).
- [ ] Keep them organized and readily available.

17. Sensitive Data & Children's Data

- [ ] Enforce special handling for sensitive personal data.

- For all the sensitive categories, ensure enhanced protections (like health, religious, biometric data, credit data, genetic data, political opinions). Take consent from guardians in case of processing children's data.
  - [ ] Collect only the minimum personal data necessary.
  - [ ] Prohibit the use of sensitive data for marketing purposes.
  - [ ] Obtain explicit consent.
  - [ ] pply stronger security and limited access.
  - [ ] Obtain consent from legal guardian (in case of children's data).
  - [ ] Apply enhanced protection of the data and limit processing (in case of children's data).

SharkStriker

300, Delaware Ave. Suite 210 402
Wilmington, DE 19801

+1 925 5321900

sales@sharkstriker.com

www.sharkstriker.com