KAT-C CONSULTING

Free Data Privacy Workbook

Your personal data is valuable. Companies, hackers, and even governments seek to collect, use, or sell your information. Protecting your privacy helps prevent identity theft, financial fraud, and unwanted surveillance.

WORKBOOK

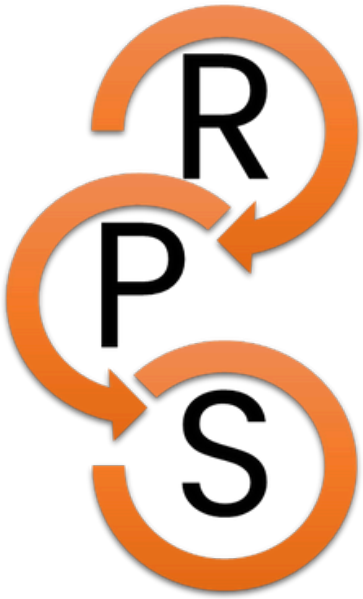
WHY DATA PRIVACY MATTERS

This guide provides practical steps to improve your data security, including:

- Understanding Legal Obligations Under the Data Protection Act (DPA)
- Steps to Secure Sensitive Customer Information
- Practical Tips for Employee Training on Data Protection
- Case Studies
- Data Privacy Checklist
- Data Privacy Workbook

DPA Compliance Frameworks

Obligations of a Personal Information Controller or Processor



UPHOLD THE RIGHTS OF DATA SUBJECTS

ADHERE TO DATA PRIVACY PRINCIPLES

IMPLEMENT SECURITY MEASURES

Understanding Your Legal Obligations Under the DPA

The Data Protection Act (DPA) is a law designed to protect individuals' personal data. The following are your core obligations as an organization under the DPA:

- **Data Collection:** Only collect data that is necessary for your operations. Ensure you inform customers about why you are collecting their data and how it will be used.
- **Data Security:** Ensure that you have appropriate technical and organizational measures in place to prevent unauthorized access or loss of data.
- **Data Access and Portability:** Customers have the right to access their personal data, request corrections, and even move it to another service if they choose.
- **Data Retention:** Do not keep customer data for longer than necessary. Define and enforce retention policies.
- **Accountability:** You must ensure that data protection is embedded within your operations, from the moment you collect data until you process or delete it.

Action Steps:

- Familiarize yourself with the specific provisions of the DPA applicable to your region or industry.
- Appoint a Data Protection Officer (DPO) if necessary, depending on the size of your organization.

Understanding Your Legal Obligations Under the DPA

Data privacy laws exist to protect individuals, businesses and organizations from data misuse. The Data Protection Act (DPA) outlines your responsibilities when handling personal information.

Date: / /

List 3 key points you business needs to learn about the Data Protection Act (DPA):

Case Study: Data Breach Due to Non-Compliance
A small retail company failed to properly secure customer data, leading to a breach that exposed personal information. Due to non-compliance with the DPA, the company faced legal penalties and loss of customer trust. What could they have done differently?

Data Mapping & Inventory

Date: / /

List all the personal data your business collects, processes, stores, or shares.

What data do you collect?	
Where is it stored?	
Who has access to it?	

Identify 2 areas where customer data security can be improved in your organization:

Consent Management

Date: / /

Document how you obtain and manage consent

Checklist:

- [ ] Do you clearly explain why you are collecting someone's data?
- [ ] Do you use simple words when asking for permission (no legal jargon)?
- [ ] Do people have a real choice to say yes or no?
- [ ] Is permission (consent) collected before collecting personal data?
- [ ] Do you keep a record of when and how people gave consent (e.g., time, method)?
- [ ] Can people easily take back their consent (unsubscribe or opt out)?
- [ ] Do you review consent regularly (especially for long-term customers)?
- [ ] Are permission requests separate from terms and conditions?
- [ ] Do you ask permission for each type of use (e.g., marketing, sharing with partners)?
- [ ] If you collect data from minors, do you have a way to get permission from a parent or guardian?

Appointment of a Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for guiding the organization in complying with data privacy laws and serves as the main link between the organization, data subjects, and regulators

Why Appoint a DPO?
Understand the legal and compliance basis.

Appointing a DPO is important for several reasons:

- It is a **legal requirement** under the Data Privacy Act (DPA), Section 21(b), and its Implementing Rules and Regulations (IRR), Sections 50(b) and 26(a).
- It is recognized by the National Privacy Commission (NPC) as one of the Five Pillars of Compliance.
- A DPO helps establish accountability and a clear privacy leadership structure within the organization.
- The DPO ensures that compliance with data privacy laws is continuously monitored and improved.
- Having a DPO supports the development and enforcement of privacy measures, policies, and procedures.
- The DPO also serves as the official liaison between the organization and the NPC, as well as with data subjects.

DPO Qualifications and Responsibilities

Qualifications of a DPO:

1. Specialized knowledge in data privacy and protection policies
2. Reliability and expertise in relevant laws and regulations
3. Understanding of the organization's data processing activities
4. Familiarity with the organization's sector or field

Duties and Responsibilities:

1. Monitor compliance with the DPA, NPC issuances, and other applicable laws
2. Ensure Privacy Impact Assessments (PIAs) are conducted
3. Advise on data subject complaints and rights
4. Report security incidents and data breaches to the NPC within prescribed periods
5. Promote awareness and training on data privacy within the organization
6. Advocate for privacy-by-design in policies, projects, and programs
7. Act as the contact person between the organization, data subjects, and regulatory authorities
8. Coordinate and cooperate with the NPC and other relevant authorities

Appointing a DPO

Worksheet:

Item	Details
DPO Name	
Appointment Date	
Contact Information	
Background/Expertise	
Sector Knowledge	

Privacy Impact Assessment (PIA)

A Privacy Impact Assessment (PIA) is a process to evaluate and manage the impacts of a program, system, or project on privacy.

Checklist:

- [ ] Identify the personal data to be collected and processed
- [ ] Determine the legal basis for data processing
- [ ] Assess the necessity and proportionality of data processing
- [ ] Identify potential privacy risks and their impact
- [ ] Consult relevant stakeholders (internal and external)
- [ ] Identify and evaluate existing security controls
- [ ] Propose additional mitigation strategies for identified risks
- [ ] Define procedures for monitoring, updating, and reviewing the PIA
- [ ] Ensure documentation of all findings and decisions
- [ ] Obtain approval from the DPO or relevant authority

PIA Documentation

Date: / /

Worksheet:

Component	Notes
Project Description	
Data Involved	
Purpose of Processing	
Potential Risks	
Stakeholder Feedback	
Mitigation Actions	
Review Schedule	

Training & Awareness

Promote data privacy awareness within the organization.

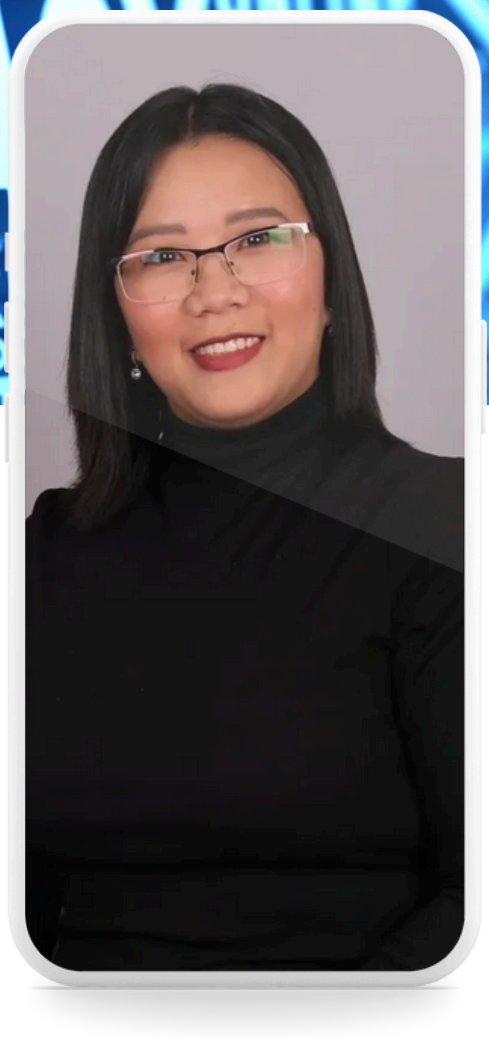
- [ ] Conduct regular data privacy training for all employees
- [ ] Include privacy orientation in onboarding for new hires
- [ ] Provide role-specific privacy training (e.g., for IT, HR, marketing)
- [ ] Distribute data privacy materials (e.g., posters, infographics, FAQs)
- [ ] Consult relevant stakeholders (internal and external)
- [ ] Conduct awareness campaigns during Privacy Awareness Week
- [ ] Maintain records of all training and awareness activities
- [ ] Evaluate effectiveness of training through feedback or assessments

Notes:

- Training should be aligned with the organization's data protection policies and tailored to the specific roles and responsibilities of employees.
- Refresher sessions should be scheduled annually or when there are updates to privacy laws or internal policies.
- Feedback forms or short quizzes can be used to assess participant understanding and improve future sessions.
- Documentation of training attendance and materials used should be kept for audit and compliance purposes.
- Consider integrating real-life case studies or recent data breach news to emphasize relevance and risks.

Compliance Framework Summary

Pillar	Compliance Action
1. Rights of Data Subjects	Document and respect SARs, corrections, erasures, etc.
2. Data Privacy Principles	Ensure transparency, legitimate purpose, proportionality
3. Security Measures	Implement appropriate technical and organizational safeguards
4. Breach Management	Maintain and practice breach response procedures
5. Accountability	Assign roles, appoint a DPO, keep documentation



Thank you!

You've taken the first step towards stronger data privacy! Thank you for downloading the **Free Data Privacy Workbook** of **Kat-C Data Privacy Business and Consulting Inc**. Now, let's keep the momentum going:

✅ **Stay Updated:** Check our website regularly for new articles and insights. Follow us on social media for quick tips and reminders.

✅ **Stay Educated:** Share this workbook and its valuable information with colleagues, friends, and family. Let's build a more privacy-conscious community together.

Atty. Krishna Aira Tana-Caguia

T: +(63)9955389250

E: inquiry@katcdataprivacy.com

L: 123 Anywhere St., Any City