DATA PROTECTION AND PRIVACY POLICY

sbPowerDev

First Drafted and Implemented for sbPowerDev, India:
31st January 2021

Revised to Include sbPowerDev, Singapore:
1st April 2023

Revisions and Updates:
31st January 2022
31st January 2023
1st April 2023
31st January 2024

Any queries / concern regarding policy should be sent to
contactus@sbpowerdev.com

Contents

DATA PROTECTION & PRIVACY POLICY

1. Introduction

sbPowerDev is committed to safeguarding personal data and ensuring compliance with data protection regulations such as GDPR, PDPA, and India's IT Act. This policy establishes a framework for managing data protection and privacy within our organization.

2. Scope

This policy applies to all employees, contractors, and third-party partners of sbPowerDev, covering all personal data processed by the company, regardless of location or format.

3. Key Principles

1. **Lawfulness, Fairness, and Transparency:**
    - Personal data must be processed lawfully, fairly, and transparently.
    - sbPowerDev will inform individuals about data collection purposes and obtain their consent where required.
2. **Purpose Limitation:**
    - Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
3. **Data Minimization:**
    - Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
4. **Accuracy:**
    - Personal data must be accurate and kept up-to-date.
    - Inaccuracies should be rectified or erased without delay.
5. **Storage Limitation:**
    - Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary.
6. **Integrity and Confidentiality:**
    - Personal data must be processed in a manner that ensures its security, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage.

4. Roles and Responsibilities

4.1 Core Team (Administrators & Policy Implementers)

- **Oversee Compliance:** Ensure compliance with data protection laws and policies across sbPowerDev.
- **Data Subject Requests:** Handle requests from data subjects regarding their rights under data protection laws.
- **Data Protection Training:** Conduct data protection training and awareness programs.
- **Manage Independent Projects:** Ensure that independent projects like Go-To Card have their own data protection policies that align with sbPowerDev's standards.

4.2 Employees and Contractors

- **Comply with Policies:** Follow all data protection policies and procedures.
- **Report Incidents:** Immediately report any data breaches or vulnerabilities to the Core Team.
- **Protect Data:** Handle personal data with care and only for authorized purposes.

4.3 Third-Party Partners

- **Adhere to Policies:** Comply with sbPowerDev's data protection policies and procedures.
- **Protect Shared Data:** Ensure that data shared with third parties is protected according to sbPowerDev's standards.
- **Cooperate with Audits:** Participate in data protection assessments and audits as required.

5. Data Collection and Processing

- **Consent:** Obtain explicit consent from data subjects where required.
- **Data Collection:** Collect personal data only for legitimate business purposes.
- **Data Processing:** Ensure that data processing aligns with the purposes for which data was collected.

6. Data Subject Rights

sbPowerDev recognizes the rights of data subjects under applicable data protection laws, including the rights to:

- **Access:** Request access to personal data held about them.
- **Rectification:** Request corrections to inaccurate or incomplete data.
- **Erasure:** Request the deletion of personal data when it is no longer necessary.
- **Restriction:** Request restrictions on the processing of their data.
- **Data Portability:** Request transfer of their data to another organization.
- **Objection:** Object to data processing based on legitimate interests or direct marketing.

7. Data Security Measures

- **Encryption:** Use encryption to protect personal data both in transit and at rest.
- **Access Control:** Limit access to personal data to authorized personnel only.
- **Regular Audits:** Conduct regular audits to assess data protection compliance and security measures.

8. Data Breach Response

- **Incident Reporting:** Establish procedures for reporting and managing data breaches promptly.
- **Response Plan:** Implement a data breach response plan to contain and mitigate breaches.
- **Notification:** Notify affected data subjects and authorities as required by law.

9. Compliance and Monitoring

- **Legal Compliance:** Ensure compliance with applicable data protection laws and regulations.
- **Policy Review:** Regularly review and update the Data Protection and Privacy Policy to reflect changes in laws or business practices.
- **Monitoring:** Implement monitoring systems to ensure ongoing compliance.

10. Training and Awareness

- **Regular Training:** Provide regular data protection training and awareness programs for all employees.
- **Policy Updates:** Communicate updates to data protection policies and procedures regularly.

11. Enforcement

- **Disciplinary Actions:** Violations of this policy may result in disciplinary action, up to and including termination of employment or contractual agreements.
- **Compliance:** All employees and partners are expected to comply with the policy and report any suspected violations promptly.

12. Independent Projects

- **Independent Data Policies:** Independent projects such as Go-To Card must maintain their own data protection policies, aligned with sbPowerDev's standards.
- **Oversight:** The Core Team is responsible for ensuring that independent projects adhere to these standards and that their policies are reviewed annually.

13. Governing Law

This policy shall be governed by and construed in accordance with the laws of India and Singapore, where applicable.

14. Appendices

- **Appendix A:** Data Collection and Consent Procedures
- **Appendix B:** Data Processing and Storage Guidelines
- **Appendix C:** Data Security Measures
- **Appendix D:** Data Breach Response Plan
- **Appendix E:** Data Subject Rights Management

APPENDIX A: DATA COLLECTION AND CONSENT PROCEDURES

A.1 Purpose

This appendix provides detailed procedures for collecting personal data and obtaining consent, ensuring compliance with data protection laws.

A.2 Data Collection Process

1. **Identify Data Needs:**
    - Determine the specific personal data required for business purposes.
    - Ensure data collection aligns with the principles of data minimization.
2. **Inform Data Subjects:**
    - Provide clear information about the data collection purpose, usage, and storage.
    - Use privacy notices and consent forms where applicable.
3. **Collect Data:**
    - Use secure methods for data collection, such as encrypted forms or secure file transfers.
    - Store data in designated, secure systems.

A.3 Obtaining Consent

1. **Explicit Consent:**
    - Obtain explicit consent for data processing activities that require it.
    - Use consent forms that are clear, concise, and easily understandable.
2. **Recording Consent:**
    - Maintain records of consent obtained, including date, method, and specific purposes.
    - Use tools like Microsoft Forms to manage consent documentation.
3. **Withdraw Consent:**
    - Provide data subjects with the ability to withdraw consent at any time.
    - Implement procedures to honor withdrawal requests promptly.

APPENDIX B: DATA PROCESSING AND STORAGE GUIDELINES

B.1 Purpose

This appendix outlines guidelines for processing and storing personal data securely and efficiently.

B.2 Data Processing Procedures

1. **Purpose Alignment:**
    - Ensure all data processing aligns with the original purposes of data collection.
    - Avoid processing data for purposes that are incompatible with the original intent.
2. **Data Minimization:**
    - Limit data processing to what is necessary for achieving business objectives.
    - Regularly review and delete unnecessary data.
3. **Automated Processing:**
    - Implement safeguards for automated data processing, including profiling.
    - Ensure transparency and accountability in automated decision-making.

B.3 Data Storage Practices

1. **Secure Storage:**
    - Store personal data in secure, access-controlled environments.
    - Use encryption and access logs to protect stored data.
2. **Retention Periods:**
    - Define and adhere to data retention periods based on business needs and legal requirements.
    - Implement procedures for secure deletion or anonymization of data no longer needed.
3. **Backup and Recovery:**
    - Ensure regular backups of critical data to prevent loss.
    - Test backup systems periodically for effectiveness.

APPENDIX C: DATA SECURITY MEASURES

C.1 Purpose

This appendix provides specific measures for protecting personal data using security tools and best practices.

C.2 Encryption Practices

1. **Data in Transit:**
    - Use TLS/SSL encryption for data transmitted over the internet.
    - Implement secure email protocols like S/MIME or PGP.
2. **Data at Rest:**
    - Encrypt sensitive data stored on servers and devices using AES-256.
    - Use BitLocker on Windows 10 Pro devices for full-disk encryption.

C.3 Access Control Measures

1. **Role-Based Access:**
    - Implement role-based access controls (RBAC) to restrict data access based on job responsibilities.
    - Regularly review and update access permissions.
2. **Multi-Factor Authentication (MFA):**
    - Enable MFA for all critical systems and applications.
    - Use Microsoft 365 MFA features to enhance security.

C.4 Monitoring and Auditing

1. **Regular Audits:**
    - Conduct regular audits of data access and processing activities.
    - Use audit logs to identify unauthorized access or anomalies.
2. **Monitoring Tools:**
    - Deploy monitoring tools to detect and respond to security threats in real-time.
    - Use Microsoft Defender for Endpoint to monitor devices and networks.

APPENDIX D: DATA BREACH RESPONSE PLAN

D.1 Purpose

This appendix outlines the response plan for managing data breaches effectively.

D.2 Breach Response Phases

1. **Identification:**
    - Use monitoring tools to detect data breaches promptly.
    - Analyze logs from Microsoft 365 and other systems for anomalies.
2. **Containment:**
    - Isolate affected systems to prevent further damage.
    - Use Microsoft Defender ATP to quarantine threats.
3. **Eradication:**
    - Remove malware and unauthorized access.
    - Apply security patches and updates.
4. **Recovery:**
    - Restore systems to normal operation.
    - Use backups to recover lost data.
5. **Notification:**
    - Notify affected data subjects and regulatory authorities as required by law.
    - Provide detailed information about the breach and mitigation measures.
6. **Lessons Learned:**
    - Conduct post-incident reviews to identify areas for improvement.
    - Update policies and training based on findings.

APPENDIX E: DATA SUBJECT RIGHTS MANAGEMENT

E.1 Purpose

This appendix provides procedures for managing data subject rights requests efficiently.

E.2 Rights Request Handling

1. **Access Requests:**
    - Verify the identity of the data subject before fulfilling access requests.
    - Provide requested data in a structured, commonly used, and machine-readable format.
2. **Rectification and Erasure:**
    - Correct inaccurate data upon request and document changes.
    - Erase data when requested, provided no legal obligations require retention.
3. **Restriction and Objection:**
    - Implement procedures to restrict data processing upon request.
    - Acknowledge and respect objections to data processing for direct marketing purposes.
4. **Data Portability:**
    - Facilitate the transfer of personal data to other organizations at the request of data subjects.
5. **Response Timelines:**
    - Respond to data subject rights requests within 30 days.
    - Document all requests and responses for auditing purposes.