



Data Privacy Policy

Version: 2.0

Effective Date: 01/04/22

Last Revised: 01/04/23

Next Review Date: 01/04/24

Approval: Bhushan Patil

Overview:

This document outlines Ausha Digital Pvt. Ltd. [ADPL] Data Privacy Policy, encompassing the entire lifecycle of personal data from collection to disposal.

Personal Data Collection:

- Purpose of Collection:
 - Clearly define the purpose for collecting personal data and ensure it aligns with lawful and legitimate business interests.
- Consent:
 - Obtain explicit consent from individuals before collecting their personal data, clearly explaining the purpose, usage, and duration of data storage.
- Sensitive Data:
 - Establish specific procedures for the collection and handling of sensitive personal data, such as health information or financial data.

Data Storage:

- Security Measures:
 - Implement robust data storage security measures, including encryption, pseudonymization, and access controls, to protect personal data from unauthorized access.
- Third-Party Data Storage:
 - Clearly define the standards and security measures when personal data is stored by third-party vendors or partners. Ensure third parties adhere to the same level of security standards.
- Data Localization:
 - Specify the geographical locations where personal data may be stored and processed.



Data Usage:

- Limitation of Usage:
 - Specify the purposes for which personal data is collected and ensure it is used only for those purposes. Any changes in data usage require explicit consent.
- Data Minimization:
 - Collect only the minimum amount of personal data necessary for the intended purpose. Regularly review and minimize data holdings.
- Profiling:
 - Clearly define policies around automated profiling, ensuring transparency and providing opt-out options for individuals.

Access Controls:

- User Access:
 - Implement and regularly review access controls to restrict access to personal data based on job responsibilities.
- Authentication:
 - Enforce strong authentication mechanisms to ensure only authorized personnel can access personal data.
- Data Portability:
 - Establish procedures for individuals to request and receive a copy of their personal data in a commonly used and machine-readable format.

Data Breach Response:

- Reporting:
 - Establish a clear process for reporting and responding to data breaches promptly, including a designated Data Privacy Officer.
- Communication:
 - Define procedures for communicating data breaches to affected individuals, regulators, and other stakeholders as required by applicable laws.
- Remediation:
 - Specify steps for remediation following a data breach, including reviewing and improving security measures.

Retention:

- Data Retention Period:
 - Clearly define the retention period for personal data, considering legal requirements and business needs.



- Data Archiving:
 - Establish procedures for archiving data that is no longer actively used but must be retained for compliance or historical purposes.

Destruction:

- Secure Disposal:
 - Specify secure methods for the destruction of personal data when it reaches the end of its retention period.
- Data Disposal Logs:
 - Maintain logs of data disposal activities, including dates and methods used.

Employee Training:

- Data Privacy Training:
 - Provide comprehensive training to employees on data privacy policies, procedures, and their role in safeguarding personal data.
- Awareness Programs:
 - Conduct regular awareness programs to keep employees informed about evolving data privacy concerns and best practices.

Document Management Controls:

- Periodic Review/Revision:
 - Conduct periodic reviews and revisions of this policy, ensuring it remains aligned with legal and organizational requirements.
- Defined Owner:
 - The Data Privacy Officer [Name and Position] is responsible for the ownership and enforcement of this policy.
- Circulation to Relevant Stakeholders:
 - Circulate this policy to all employees, contractors, and relevant stakeholders who handle personal data.
- Document Classification Labeling:
 - Classify and label this document according to its sensitivity level, ensuring proper handling and access controls.

For AUSA DIGITAL PVT. LTD.


DIRECTOR

For AUSA DIGITAL PVT. LTD.

आशा ड्याडगाव
DIRECTOR