Data Privacy & Personal Data Protection Policy (POL-02)

	Function	Name	Sign/Date
Prepared by			
Reviewed by			
Approved By			

Distribution List

Department Name	Copy No.	Checkbox
		☐
		☐
		☐
		☐
		☐
		☐
		☐
		☐

Document History

Issue No.	Issue Date	Changed Occurred/ Page Number	Res. Person

1. Purpose:

The purpose of this Data Privacy and Personal Data Protection Policy is to establish the principles and requirements governing the collection, processing, use, storage, sharing, retention, and disposal of Personal Data by **Asbab Technical Company**.

This policy aims to:

1.1 Ensure that Personal Data is processed lawfully, fairly, transparently, and for legitimate and specified purposes.

1.2 Protect the privacy and rights of Data Subjects in relation to their Personal Data.

1.3 Ensure that only the minimum Personal Data necessary for the intended purpose is collected and processed.

1.4 Establish appropriate responsibilities and controls for the protection of Personal Data throughout its lifecycle.

1.5 Ensure compliance with the applicable laws, regulations, and requirements governing Personal Data protection in the Kingdom of Saudi Arabia.

1.6 Establish a framework for responding to Data Subject requests, complaints, and Personal Data breaches.

1.7 Promote privacy considerations when designing or changing processes, systems, products, or services that involve Personal Data.

2. Scope

2.1 This policy applies to all Personal Data collected, received, processed, stored, transferred, shared, or otherwise handled by **Asbab Technical Company**.

2.2 This policy applies to Personal Data processed through electronic systems as well as physical records.

2.3 This policy applies to all employees, management, contractors, consultants, temporary personnel, and other individuals who process or have access to Personal Data on behalf of the Company.

2.4 This policy also applies to relevant suppliers, service providers, processors, and other third parties that process Personal Data on behalf of the Company.

2.5 The policy applies throughout the Personal Data lifecycle, including collection, processing, use, storage, sharing, retention, and destruction.

2.6 Where Personal Data is processed on behalf of customers or other parties, applicable contractual and legal requirements shall also be considered.

3. Definitions and Abbreviations

3.1 Personal Data

Any data, regardless of its source or form, that may lead to identifying an individual specifically, or that may directly or indirectly make it possible to identify an individual.

3.2 Data Subject

The individual to whom the Personal Data relates.

3.3 Processing

Any operation performed on Personal Data, including collection, recording, storage, organization, modification, retrieval, use, disclosure, sharing, transmission, or destruction.

3.4 Controller

The entity that determines the purpose and manner of processing Personal Data.

3.5 Processor

The entity that processes Personal Data on behalf of the Controller.

3.6 Consent

The explicit and informed permission given by the Data Subject for the processing of their Personal Data where consent is required as a legal basis.

3.7 Personal Data Breach

A breach that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

3.8 Sensitive Personal Data

Personal Data that is subject to enhanced protection requirements under applicable laws and regulations.

3.9 PDPL

Personal Data Protection Law of the Kingdom of Saudi Arabia.

4. Privacy Principles:

4.1 Lawfulness, Fairness and Transparency

Personal Data shall be processed in accordance with applicable laws and regulations and in a fair and transparent manner.

4.2 Purpose Limitation

Personal Data shall be collected and processed for specified, legitimate, and authorized purposes.

4.3 Data Minimization

Personal Data collected shall be adequate, relevant, and limited to what is necessary for the intended purpose.

4.4 Accuracy

Reasonable measures shall be taken to ensure that Personal Data is accurate, complete, and kept up to date where necessary.

4.5 Storage Limitation

Personal Data shall not be retained for longer than necessary to fulfill the purpose for which it was collected, unless retention is required or permitted by applicable requirements.

4.6 Confidentiality and Security

Personal Data shall be protected against unauthorized access, disclosure, alteration, loss, destruction, or other unauthorized processing.

4.7 Accountability

The Company shall maintain appropriate measures to demonstrate compliance with applicable Personal Data protection requirements.

4.8 Privacy by Design

Privacy and Personal Data protection requirements shall be considered when designing or modifying relevant processes, systems, and services.

---

5. Roles and Responsibilities

5.1 Top Management

Top Management shall:

- Approve and support this policy.
- Provide appropriate resources for Personal Data protection.
- Ensure that significant privacy risks are appropriately addressed.
- Support compliance with applicable Personal Data protection requirements.

5.2 Data Protection / Privacy Function

The designated Data Protection or Privacy function shall, where applicable:

- Coordinate implementation of this policy.
- Monitor compliance with Personal Data protection requirements.
- Support privacy risk assessments.
- Coordinate Data Subject requests.
- Support the management of Personal Data breaches.
- Maintain relevant privacy documentation and records.
- Provide privacy awareness and guidance to personnel.

5.3 Information Owners / Relevant Functions

Relevant functions shall:

- Identify Personal Data under their responsibility.
- Ensure that Personal Data is processed only for authorized purposes.
- Apply appropriate retention and access requirements.
- Support the accuracy and protection of Personal Data.

5.4 Employees and Contractors

Employees and contractors shall:

- Comply with this policy.
- Access Personal Data only when authorized and required for their responsibilities.
- Protect Personal Data against unauthorized disclosure or use.
- Report suspected Personal Data breaches or privacy violations promptly.

5.5 Third Parties and Processors

Third parties processing Personal Data on behalf of the Company shall:

- Comply with applicable contractual and privacy requirements.
- Process Personal Data only for authorized purposes.
- Implement appropriate protection measures.
- Notify the Company of relevant Personal Data breaches or incidents.

6. Collection of Personal Data:

6.1 Personal Data shall be collected only when there is a legitimate and authorized purpose for its collection.

6.2 The Company shall avoid collecting Personal Data that is unnecessary for the intended purpose.

6.3 Appropriate measures shall be taken to ensure that the method of collecting Personal Data is lawful, clear, secure, and appropriate to the circumstances.

6.4 Where Personal Data is collected directly from the Data Subject, the Data Subject shall be provided with appropriate privacy information in accordance with applicable requirements.

6.5 Where Personal Data is collected indirectly, the Company shall consider the applicable legal and regulatory requirements governing such collection.

6.6 Personal Data collected through websites, applications, forms, electronic communications, physical documents, or other channels shall be handled in accordance with this policy.

7. Purpose and Use of Personal Data:

7.1 Personal Data shall only be processed for specified and legitimate purposes.

7.2 Personal Data shall not be used for purposes that are incompatible with the purpose for which it was collected unless permitted by applicable requirements.

7.3 Access to and use of Personal Data shall be limited to authorized personnel with a legitimate business need.

7.4 Where processing is based on consent, the Company shall maintain appropriate records of consent where required.

7.5 Where the applicable legal basis for processing changes or ceases to apply, the relevant processing shall be reviewed and appropriate action shall be taken.

8. Legal Basis and Consent:

8.1 The Company shall identify an appropriate legal basis for processing Personal Data before processing takes place, in accordance with applicable requirements.

8.2 Where consent is required, it shall be obtained through an appropriate method and shall be sufficiently informed and clear.

8.3 Where applicable, Data Subjects shall be informed of the purposes for which their Personal Data is collected and processed.

8.4 Where consent is relied upon as the legal basis for processing, the Company shall maintain appropriate records demonstrating such consent where required.

8.5 Where applicable, Data Subjects shall be provided with mechanisms for exercising their rights regarding consent in accordance with applicable requirements.

9. Privacy Notices and Transparency:

9.1 The Company shall provide appropriate privacy information to Data Subjects in accordance with applicable requirements.

9.2 Privacy notices shall, as applicable, explain:

- The identity and contact details of the relevant entity.
- The Personal Data being collected.
- The purpose of collection and processing.
- The legal basis for processing.
- The methods of collection.
- How Personal Data is processed and stored.
- Relevant retention and destruction arrangements.
- Whether Personal Data will be shared with other parties.
- Relevant Data Subject rights.

- How Data Subjects can exercise their rights.
- How privacy-related inquiries and complaints can be submitted.

9.3 Privacy notices shall be reviewed and updated when there are material changes to Personal Data processing activities.

10. Data Subject Rights:

10.1 The Company shall provide appropriate mechanisms for Data Subjects to exercise their rights in accordance with applicable laws and regulations.

10.2 Such rights may include, as applicable:

- The right to be informed.
- The right to access Personal Data.
- The right to obtain a copy of Personal Data.
- The right to request correction or completion of Personal Data.
- The right to request destruction of Personal Data where applicable.
- The right to withdraw consent where processing is based on consent, subject to applicable requirements.
- Any other rights provided under applicable laws and regulations.

10.3 Requests from Data Subjects shall be appropriately verified, recorded, assessed, and responded to within the applicable timeframe.

10.4 Where a request cannot be fulfilled, the reason shall be documented and communicated to the Data Subject where required.

11. Personal Data Accuracy:

11.1 The Company shall take reasonable measures to ensure that Personal Data is accurate, complete, and up to date where necessary.

11.2 Personnel responsible for Personal Data shall correct or update inaccurate information when identified or when a valid request is received.

11.3 Data Subjects shall be provided with appropriate mechanisms to request correction of their Personal Data.

12. Personal Data Security:

12.1 Appropriate technical and organizational measures shall be implemented to protect Personal Data against unauthorized access, disclosure, alteration, loss, destruction, or misuse.

12.2 Access to Personal Data shall be based on legitimate business requirements and the principle of least privilege.

12.3 Personal Data shall be protected during storage and transmission according to its sensitivity and associated risks.

12.4 Appropriate controls shall be applied to Personal Data stored in electronic and physical formats.

12.5 Personal Data security requirements shall be considered when selecting systems, services, suppliers, and technologies that process Personal Data.

12.6 Security measures shall be periodically reviewed and updated according to changes in risks and threats.

13. Sharing and Disclosure of Personal Data:

13.1 Personal Data shall not be shared or disclosed unless there is an authorized and lawful basis for such sharing.

13.2 Before sharing Personal Data with another party, the Company shall consider:

- The purpose of sharing.
- The legal basis.
- The type and sensitivity of Personal Data.
- The identity and reliability of the receiving party.
- Applicable contractual requirements.
- Appropriate security and privacy safeguards.

13.3 Third parties receiving Personal Data shall only process it for authorized purposes and in accordance with applicable requirements.

13.4 Where appropriate, contractual agreements shall include requirements relating to confidentiality, security, privacy, processing, breach notification, and return or destruction of Personal Data.

14. Personal Data Processors and Third Parties:

14.1 The Company shall assess relevant privacy and security risks before engaging third parties that process Personal Data on its behalf.

14.2 Appropriate contractual arrangements shall be established with relevant Processors.

14.3 Processors shall process Personal Data only according to authorized instructions and applicable requirements.

14.4 The Company shall take reasonable measures to monitor the Processor's compliance with relevant privacy and security requirements.

14.5 Third-party access to Personal Data shall be limited to what is necessary for the agreed services.

15. Transfer of Personal Data Outside the Kingdom:

15.1 Transfers or disclosures of Personal Data outside the Kingdom of Saudi Arabia shall be carried out only in accordance with applicable laws, regulations, and requirements.

15.2 Before transferring Personal Data outside the Kingdom, the Company shall assess the applicable requirements, risks, safeguards, and legal basis for the transfer.

15.3 Appropriate safeguards and contractual arrangements shall be implemented where required.

15.4 Cross-border transfers shall be documented and monitored where required.

16. Retention and Destruction:

16.1 Personal Data shall be retained only for as long as necessary to fulfill the purpose for which it was collected, subject to applicable legal, regulatory, contractual, and business requirements.

16.2 Retention periods shall be defined where appropriate based on the type and purpose of the Personal Data.

16.3 When Personal Data is no longer required and there is no applicable requirement to retain it, it shall be securely destroyed or anonymized, as appropriate.

16.4 Destruction methods shall prevent unauthorized recovery or access to the Personal Data.

16.5 Personal Data retained for legal, regulatory, contractual, or dispute-related purposes shall be appropriately protected during the retention period.

17. Personal Data Breach Management:

17.1 The Company shall maintain a process for identifying, assessing, documenting, managing, and responding to Personal Data breaches.

17.2 Employees and relevant third parties shall immediately report suspected or actual Personal Data breaches.

17.3 Personal Data breaches shall be assessed to determine their nature, scope, impact, and potential risks to Data Subjects.

17.4 Where required, the Company shall notify the competent authority and/or affected Data Subjects within the applicable regulatory timeframes.

17.5 Appropriate measures shall be taken to contain, mitigate, and remediate Personal Data breaches.

17.6 Lessons learned from Personal Data breaches shall be used to improve privacy and security controls.

18. Privacy Impact Assessment:

18.1 Privacy risks shall be assessed when introducing or significantly changing processes, systems, services, technologies, or activities involving Personal Data, where required or appropriate.

18.2 A Privacy Impact Assessment (PIA) or equivalent assessment shall be conducted where the processing is likely to result in significant privacy risks.

18.3 The assessment shall consider, as applicable:

- The nature and purpose of processing.
- Categories of Personal Data.
- Categories of Data Subjects.
- Potential privacy risks.
- Security measures.
- Data sharing.
- Retention.

- Cross-border transfers.
- Measures to reduce identified risks.

18.4 Identified privacy risks shall be addressed before the relevant processing activity is implemented where reasonably practicable.

19. Records and Documentation:

19.1 The Company shall maintain appropriate records and documentation relating to Personal Data processing activities, where required.

19.2 Relevant records may include:

- Personal Data inventories.
- Records of Processing Activities (RoPA), where required.
- Privacy notices.
- Consent records, where applicable.
- Data Subject requests.
- Data sharing arrangements.
- Processor agreements.
- Retention schedules.
- Privacy risk assessments.
- Personal Data breach records.
- Relevant training and awareness records.

19.3 Privacy records shall be maintained, protected, and made available to authorized personnel as required.

20. Privacy Awareness and Training:

20.1 Personnel who handle Personal Data shall receive appropriate privacy and Personal Data protection awareness and training.

20.2 Training shall be provided upon joining the Company and periodically thereafter, based on roles and responsibilities.

20.3 Personnel with specific responsibilities involving Personal Data shall receive additional role-specific guidance where necessary.

20.4 Awareness activities shall reinforce the importance of confidentiality, appropriate data handling, privacy rights, incident reporting, and compliance with this policy.

21. Complaints and Privacy Requests:

21.1 The Company shall provide appropriate channels for Data Subjects to submit privacy-related requests, inquiries, or complaints.

21.2 Requests and complaints shall be recorded, assessed, and handled by authorized personnel.

21.3 The identity of the requester shall be appropriately verified before providing or modifying Personal Data.

21.4 Requests shall be handled within the timeframes and procedures required by applicable laws and regulations.

21.5 Complaints shall be investigated fairly and appropriate corrective action shall be taken where necessary.

22. Compliance, Monitoring and Review:

22.1 Compliance with this policy shall be monitored through appropriate reviews, assessments, audits, and other monitoring activities.

22.2 The Company shall monitor changes in applicable Personal Data protection laws, regulations, and regulatory guidance.

22.3 Non-compliance and identified privacy risks shall be appropriately addressed and monitored.

22.4 This policy shall be reviewed at least annually and whenever significant changes occur in:

- Applicable laws or regulations.
- Personal Data processing activities.
- Organizational structure.
- Systems or technologies.
- Business processes.
- Identified privacy risks.

22.5 The policy shall be continually improved based on assessment results, incidents, complaints, regulatory developments, lessons learned, and changes in the Company's context.

23. Policy Exceptions:

23.1 Any exception to this policy shall be formally documented, justified, risk assessed, and approved by the appropriate authority.

23.2 Exceptions shall have a defined validity period and shall be reviewed periodically.

23.3 Appropriate compensating measures shall be implemented where necessary to reduce the associated privacy risk.

24. Enforcement:

24.1 Failure to comply with this policy may result in appropriate corrective, disciplinary, contractual, or legal action in accordance with applicable requirements.

24.2 Violations involving unauthorized access, use, disclosure, transfer, modification, loss, or destruction of Personal Data shall be investigated and addressed appropriately.

24.3 Serious or repeated violations shall be escalated to the appropriate management and relevant functions.