العربية
al arabia

Privacy and Data Protection policy

1- Definitions

The following terms and expressions shall have the meaning they bear as follows unless the contrary intention appears:

The Kingdom: The Kingdom of Saudi Arabia

"The Company'' or "alarabia'': Arabian Contracting Services Co.

Laws and Regulations: The Laws and Implementing Regulations in Saudi Arabia.

Personal Data Protection Law: Personal Data Protection Law issued by the Royal decree number M/90 on 9/2/1443H corresponding to 16/9/2021.

Personal Data: Any statement - regardless of its source or form - that would lead to the identification of the individual specifically, or make identifying possible directly or indirectly, such as: name, personal identity number, addresses, contact numbers, license numbers, records, personal properties, bank account numbers, credit cards, still or moving visual images of the individual, and all other personal data.

Sensitive Data: Any personal data that includes a reference to the individual's ethnic, tribal origin, religious, philosophical, political beliefs, and if the data indicates his membership in associations or civil institutions. In addition to the criminal and security data, biometric data that identifies the identity, genetic data, credit data, health data, location data, and data indicating that the individual is unknown to one or both parents.

The competent authorities: Any entity of the competent authorities according to the laws and regulations responsible for collecting any personal data or information.

The company's servers: The servers that are under the control of the company, whether in the main headquarters, branches, or the cloud servers.

Stakeholders: Individuals or groups of individuals that have a direct or indirect stake in an organization who can affect or be affected by the organization's actions, objectives, and policies. Key stakeholders in an organization include "shareholders, Board members, Executive Management, employees, clients, creditors, banks, suppliers, local community and government".

The Company's official website:
al-arabia.com/investor-relations

2- Purpose

The company recognizes the importance of maintaining the privacy of individuals and their personal data, thus the company is committed to providing adequate protection for all information and personal data and maintaining its confidentiality, and the company is subject to the provisions of the Personal Data Protection law and its implementing regulations, which established the legal basis for processing personal data, including processing data over the Internet. The Personal Data Protection Policy was prepared to provide the highest standards of privacy and protection, and established the principles for processing (for example, collection and use, disclosure, transfer, sharing, storage and integration and destruction) of all relevant information and personal data. This policy assists alarabia to protect personal data and comply with applicable laws and regulations.

3- Scope

This policy applies to all employees, clients, suppliers, investors and applies to the Arabian Contracting Services Co. and all its branches and subsidiaries.

4- Data to be kept confidential

The company must provide the necessary protection for the personal data of its clients, suppliers, employees, and investors and not disclose this data for any reason except with prior consent. This data includes personal identities, information, employee records, health data, data on salaries and other financial benefits, sensitive data, and the company's access to this information must be for business purposes and not to be accessed by anyone other than authorized persons.

5- Limit of data collection

The company has the right to collect data, however the collected data shall only be the necessary specific data to achieve the purpose which it was collected for.

6- Disclosure of personal data

- If the owner of the personal data agrees to disclose the data in accordance with the provisions of the laws and regulations.
- If the personal data has been collected from a public source.
- If the disclosure is to the competent authorities, for security purposes or to implement the provisions of another law or to meet any judicial requirements as determined by the laws and regulations.
- If the disclosure is necessary to protect public health and safety.

7- Training

The necessary training is provided to all employees of the company at various job levels, on the importance of protecting their personal data or that of others, as mentioned in this policy.

8- Electronic Data Protection

The company is keen to provide the highest level of protection for the data stored electronically, and invests in the best and latest software for each of:

- Hacking and cyberattacks Protection programs.
- Phishing protection programs.
- Programs to encrypt data stored in the company's servers.
- Programs that provide multi-factor authentication to access email data or other data stored on the company's servers.

The company is committed to disclose in its annual report the latest investments in data protection, and any case of data breaches of the company servers.

9- Publication, enforcement, and amendments

This policy shall be effective and binding on the company as of the date of its approval by the Board of Directors and this policy shall be published on the company official website to enable shareholders, public and stakeholders from employees and others to view it, and this policy shall be reviewed periodically based on the recommendation of the Board of Directors, and any proposed amendments shall be presented to the Board of Directors, which shall study and review the proposed amendments and approve them.