DATA PROTECTION POLICY

Introduction

The Alrabia Investment Company and its affiliated companies hence forth referred as “company” needs to gather and use certain informations about individuals. These can include customers, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company’s data protection standards - and to comply with the law.

Why this policy exists

This data protection policy ensures the Alrabia Investment company:

- Complies with data protection law and follow good practice;

- Protects the rights of staff, customers and partners;

- Is open about how it stores and processes individual’s data;

- Protects itself from the risk of a data breach.

People, risks and responsibilities

This policy applies to:

- The head of office of the Alrabia Investment Co.;

- All branches of the Alrabia Investment Co.;

- All staff and volunteers of the Alrabia Investment Co.;

- All contractors, suppliers and other people working on behalf of the Alrabia Investment Co.;

It applies to all data that the company holds relating to identifiable individuals even if that information technically falls out of the Data Protection Act. This can include:

- Name of individuals;

- Postal addresses;

- Email addresses;

- Telephone numbers.

Data protection risks

This policy helps to protect the Alrabia Investment Co.; from some real data security risks, including:

- Breaches of confidentiality, informations being given out inappropriately;

- Falling to offer choice, all individuals should be free to choose how the company uses data relating to them;

- Reputation damage, the company could suffer it hackers successfully gained access to sensitive data.

Responsabilities

Everyone who works for or with the Alrabia Investment Co. has some responsability for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- *The Board of Directors* is ultimately responsible for ensuring that the Alrabia Investment Co.; meets its legal obligations.

The *Chief Compliance Officer*, is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues;

- Reviewing all data protection procedures and related policies, in line with an agreed schedule;

- Handling data protection questions from staff and anyone else covered by this policy;

- Dealing with request from individuals to see the data the Alrabia Investment Co., holds about them (also called “subject access requests”);

- Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.

The *IT Manager*, is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards;

- Performing regular checks and scans to ensure security hardware and software is functioning properly;

- Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services;

- Arranging data protection training and advice for the people covered by this policy;

- handling data protection questions from staff and anyone else covered by this policy.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work;

- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers;

- Alrabia Investement Co., will provide training to all employees to help them understand their responsibilities when handling data;

- Employee should keep all data secure, by taking sensible precautions and following the guidelines below;

- In particolar, strong password must be used;

- Personal data should not be disclosed to unauthorized people, either within the company or externally;

- Data should be regularly reviewed and updated it it is found to be out of date.

If no longer require, it should be deleted and disposed of.

- Employees should request help from their line manager or the Chief Compliance Officer, if they are unsure about any aspect of data protection.

Data Storage

- These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Manager. When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filling cabinet;

- Employees should make sure paper and printouts are not left where unauthorized people could see them, like on a printer;

- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees;

- If data is stored on removable media (like a CD, DVD, or Flash Drive) these should be kept locked away securely when not being used;

- Data should only be stored on designated drivers and servers and should only be uploaded to an approved cloud computing services;

- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures;

- Data should never be saved directly to laptops or other mobile devices like tablets or smartphones;

- All servers and computers containing data should be protected by approved security software (anti-virus software).

Data Use

Personal data is of no value to the Alrabia Investment Co. unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computer always locked when left unattended;

- Personal data should not be shared informally, it should never be sent by email as this form of communication is not secure;

- Data must be encrypted before transferred electronically. The IT Manager can explain how to send data to authorized external

contract;

- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Subject access requests

All individuals who are the subject of personal data held by the Alrabia Investment Co., are entitled to:

- Ask what information the company holds about them and why;

- Ask how to gain access to it;

- Be informed how to keep it up to date;

- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email.

The data subject shall receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

Disclosing data for other reason

In certain circumstances, the Data protection act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, the Alrabia Investment Co., will disclose requested data.

Providing information

The Alrabia Investment Co., aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used;

- How to exercise their rights.