DATA PRIVACY PROTECTION PROCEDURES

Policy Brief & Purpose

Our ***Data Protection company policy*** refers to the company's commitment to treat information of employees, customers, agents or other interested parties with the utmost care and confidentiality. With this policy we ensure that our company behaves in a fair and moral manner concerning the gathering, storing and handling of data. This process will be carried out with transparency and respect towards the rights of individuals who entrust it with their information.

Scope

This policy applies to all parties (employees, job candidates, customers, suppliers etc.) who provide any amount of information to the company. The policy will be followed by all employees of the company and its subsidiaries as well as contractors, consultants, partners, branches and any other external entity. Generally, it refers to anyone who is in close collaboration with the company or acts on its behalf and may need occasional access to data.

Policy elements

The company will need to obtain and process information of people that will serve its business purposes. The information may refer to any offline or online information that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

The company commits to collect this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to the company, the following rules are mandatory:

- The data will be collected fairly and for lawful purposes only
- The data will be processed by the company within its legal and moral boundaries
- The data will not be stored for more than the specified amount of time
- The data will be accurate and kept up-to-date
- The data will not be distributed to any party other than the ones agreed upon by the owner of the data (exempting legitimate requests from law enforcement authorities)
- The data will not be transferred to organizations, states or countries that do not have adequate data protection policies
- The data will not be communicated informally
- The data will be protected against any unauthorized or illegal access by internal or external parties

In addition to ways of handling the data the company has direct obligations towards people to whom the data belongs.

Specifically, the company must:

- Let people know which of their data is collected
- Inform people about how their data will be processed
- Inform people about who has access to their information
- Allow people to request the modification, erasing, reduction or correction of the data contained in the company's databases
- Have provisions in cases of lost, corrupted or compromised data

Actions & Procedures

To exercise data protection, the company is committed to:

- Develop transparent data collection procedures
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)
- Build secure networks to protect online data from cyber attacks
- Include contract clauses or communicate statements on how data will be handled
- Inform individuals of the amount of time that their data will be preserved
- Declare its data protection provisions publicly (e.g. on website)
- Ensure all concerned parties have read the policy and adhere to it
- Train employees in online privacy and security measures
- Restrict and monitor access to sensitive data
- Establish clear procedures for reporting breach of privacy or data misuse

Data collection

Informed consent is when:

- An Individual/Service User clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- And then gives their consent.

Our company will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, we will ensure that the Individual/Service User:

- Clearly understands why the information is needed
- Understands what it will be used for and what the consequences are should the Individual/Service User decide not to give consent to processing
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- Has received sufficient information on why their data is needed and how it will be used

Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made by the management