Data Protection Policy

Policy brief & purpose

Our Company Data Protection Policy refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality.

With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights, respecting the eight principles of the Act:-

Data protection principles:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
7. Appropriate technical and organisational measures shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Scope

This policy refers to all parties (employees, job candidates, customers, suppliers etc.) who provide any amount of information to us.

Who is covered under the Data Protection Policy?

1. All employees of our company and its subsidiaries must follow this policy. Contractors, consultants, partners and any other external entity are also covered.
2. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

Policy elements

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

Our company collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Our data will be:

1. The minimal amount of data required for the purpose will be collected.
2. Accurate and kept up-to-date.
3. Collected fairly and for lawful purposes only.
4. Processed by the company within its legal and moral boundaries.
5. Protected against any unauthorized or illegal access by internal or external parties. All paper records will be kept locked. All databases will be pass worded using a strong verified password using a password manager.

Our data will not be:

1. Communicated informally.
2. Not stored for more the specified amount of time assessed.
3. Transferred to organizations, states or countries that do not have adequate data protection policies'.
4. Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities).
5. In addition to ways of handling the data the company has direct obligations towards people to whom the data belongs.
6. The website does not use cookies or collect personal data.

Specifically we must:

1. Let people know which of their data is collected. All data of a personal nature is for payroll, pension, HSE and legal purposes only. Unsolicited external CV's will be responded to within one week and immediately deleted.
2. Inform people about how we'll process their data as part of their contract for employees.
3. Inform people about who has access to their information as part of their contract for employees.

4. Have provisions in cases of lost, corrupted or compromised data. All data is backed up constantly offsite encrypted. Additional backups on removable media are bit locked to secure the data.
5. Allow people to request that we modify, erase, reduce or correct data contained in our databases.

Actions

To exercise data protection we're committed to:

1. Restrict and monitor access to sensitive data.
2. Develop transparent data collection procedures.
3. Train employees in online privacy and security measures.
4. Build secure networks to protect online data from cyberattacks. All systems have anti-virus protection and firewalls where appropriate.
5. Inappropriate websites are not visited.
6. Establish clear procedures for reporting privacy breaches or data misuse.
7. Include contract clauses or communicate statements on how we handle data.
8. Establish data protection practices (document shredding/burning, secure locks for paper records, data encryption, frequent bit locked backups, constant offsite encrypted backup, access authorization etc.).
9. Our data protection provisions will appear on our website.

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.

Adopted :- 12th April 2018

To be reviewed on 12th April 2021 or when appropriate.