Munjal Kiriu Industries Private Limited

Data Protection Policy

Confidentiality Agreement

K. Saravanan	Ravee Kant Sharma	Vijay Pal Singh	Controlled copy STAMP	Revision detail	
Approved by	Checked by	Prepared by		REV.NO. 01	REV.DATE 02/07/2025

Document Control

DOCUMENT REVISION HISTORY				
Ver	**Date**	**Editor**	**Nature of Revision**	**Previous Correspondence**
1.0	**02/07/2025**	**Ravee Kant Sharma**	**First Release**	**NA**

Document Reviewers

Reviewed by	Approved by	Final Comments
Vijay Pal Singh	**Mr. K. Saravanan (MD)**	**Initial Document**

Contents

1. Purpose

MUNJAL KIRIU is committed to a policy of protecting the rights and privacy of individuals, groups, and interested parties in accordance with The Data Protection Act 1998 and Data Protection Bill 2013. The policy applies to all employees, vendors, suppliers, contractors, and other interested parties. Any breach of the Data Protection Act 1998, Data Protection Bill 2013, and IT Act 2000 or MUNJAL KIRIU Data Protection Policy is an offence, and, in that event, disciplinary processes apply.

As a legal requirement, data is protected by the Data Protection Act 1998, which came into effect on 1 March 2000. Its purpose is to protect the rights and privacy of individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent.

The Act requires us to register the fact that we hold personal data and to acknowledge the right of 'subject access' – employees, clients, and other interested parties must have the right to copies of their own data.

2. Scope

Data may be held by MUNJAL KIRIU /the company for the following purposes:

- Operational Data
- Project/Product Data
- Source Codes
- Passwords
- Account and Finance Data
- Marketing & Sales data
- Client-based data
- External Origin Data
- Obsolete data
- Administrative data
- IT Data
- Interested parties and stakeholders' data
- Employee data
- Platform Transactional Data
- And other

3. Data Protection Principles

In terms of the Data Protection Act 1998, we are the 'data controller' and 'data processor', and as such determine the purpose for which, and the way, any personal data is, or is to be, processed.

We must ensure that we have:

3.1 Fairly and lawfully processed personal data

MUNJAL KIRIU will always put Confidentiality marking as stated in Refer "ISMS Manual- MKI/ISMS/01" on paperwork, stating their intentions on processing the data, and stating if, and to whom, we intend to give the personal data. Also, provide an indication of the duration the data will be kept.

3.2 Processed for a limited purpose

We will not use data for a purpose other than those agreed upon by data subjects (clients, vendors, suppliers, contractors, and other interested parties). If the data held by us is requested by external MUNJAL KIRIU s for any reason, this will only be passed if data subjects agree, except for the client data related to the project and product. Also, external MUNJAL KIRIU s must state the purpose of processing, agree not to copy the data for further use, and sign a contract agreeing to abide by The Data Protection Act 1998 and MUNJAL KIRIU Data Protection Policy.

3.3 Adequate, relevant, and not excessive

The MUNJAL KIRIU will monitor the data held for their purposes, ensuring we hold neither too much nor too little data in respect of the projects/products/services. If the data given or obtained is excessive for such purpose, it will be immediately deleted or destroyed, or returned.

3.4 Accurate and up-to-date

We will provide our members/partners/clients with a copy of their data as per their expression and written request, where relevant. All amendments will be made immediately, and data no longer required will be deleted or destroyed. It is the responsibility of individuals and MUNJAL KIRIU to ensure the data held by us is accurate and up to date. Individuals should notify us of any changes to enable personnel records to be updated accordingly. It is the responsibility of the MUNJAL KIRIU to act upon notification of changes to data, amending them where relevant.

3.5 Not kept longer than necessary

We discourage the retention of data for longer than it is required. For Retention Refer
Refer to "MKI/ISMS/30-Data Retention Policy MUNJAL KIRIU"

3.6 Processed in accordance with the individual's rights

All individuals that the MUNJAL KIRIU holds data on have the right to:

- Be informed upon request of all the information held about them within 60 days.
- Prevent the processing of their data for the purpose of direct marketing.
- The removal and correction of any inaccurate data about them.
- Financial Compensation or any other compensation will not be provided by the company.

3.7 Secure and backed up

Appropriate technical and MUNJAL KIRIU measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of data.

The company has a login system, and our Contact Database is password-protected, admin-controlled, and online, which allows only authorized users to access personal data. Passwords on all computers are changed frequently. All personal and financial data is kept in a locked filing cabinet and can only be accessed by authorized officers. When staff members are using the laptop computers out of the office, care should always be taken to ensure that personal data on the screen is not visible to strangers.

Refer: MKI/ISMS/35-Clear Desk and Clear Screen Policy MUNJAL KIRIU"

Where expressly asked by the client, data encryption is used.

Users are required to use a protected VPN to securely access and use company laptops. This ensures secure and encrypted connections, protecting sensitive company data during transmission. VPN usage is mandatory for all remote and internal access to company resources.

Not transferred to countries unless the country has adequate protection for the individual.

Data must not be transferred to countries outside of India without the explicit consent of the individual, except when required for legitimate business purposes and in compliance with applicable data protection laws. The company takes particular care to be aware of this when publishing information on the Internet, which can be accessed from anywhere in the world. This is because transfer includes placing data on a website that can be accessed from outside the country.

4. Roles and Responsibilities

4.1 Data Protection Officer (DPO)

- Oversees the implementation and maintenance of the data protection program.
- Ensures compliance with data protection laws and regulations.
- Acts as the point of contact for data protection issues and incidents.

4.2 Information Security Team

- Implements and manages technical and MUNJAL KIRIU measures to protect data.
- Conducts regular security assessments and audits.
- Monitors compliance with the data protection policy.

4.3 Employees and Contractors

- Adhere to data protection policies and procedures.
- Report any data breaches or security incidents immediately.
- Participate in data protection training and awareness programs.

5. Data Classification

Refer to *"MKI/ISMS/01-ISMS Manual"*

6. Data Handling

Data shall be handled according to its classification level. Measures include:

- Encryption: All confidential and restricted data must be encrypted during storage and transmission.
- Access Controls: Access to data must be restricted based on the principle of least privilege.
- Data Minimization: Collect and retain only the minimum amount of data necessary for business purposes.
- Secure Disposal: Data must be securely disposed of when no longer needed, using methods such as shredding, degaussing, or secure erasure.

7. Data Security Measures

7.1 Technical Measures

- Implement firewalls, antivirus software, intrusion detection systems, and other security technologies to protect data.
- Use encryption and secure communication protocols (e.g., TLS/SSL) to protect data during transmission.

7.2 MUNJAL KIRIU Measures

- Develop and enforce data protection policies and procedures.
- Conduct regular training and awareness programs for employees and contractors.
- Perform regular security audits and risk assessments.

8. Data Breach Management

8.1 Incident Reporting:

Refer to "MKI/ISMS/22-Incident Management Procedure"

8.2 Incident Response:

Refer to "MKI/ISMS/22-Incident Management Procedure"

9. Compliance and Monitoring

- Conduct regular internal and external audits to ensure compliance with data protection laws and this policy.
- Perform regular risk assessments to identify and mitigate data protection risks.

10. Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment or contract. Legal actions may also be pursued in cases of unlawful data handling or breaches.