G TECH INFRASTRUCTURE

G-TECH INFRASTRUCTURE PRIVATE LIMITED, INDIA

DATA SHARING POLICY

A. INTRODUCTION

G-Tech Infrastructure Private Limited (G-Tech Infrastructure) ("the Company") is dedicated to advancing development outcomes through effective collaboration and data utilisation. This Data Sharing Policy ("the Policy") aims to facilitate the responsible and secure sharing of data to foster transparency, accountability, and innovation while protecting the confidentiality and integrity of sensitive information.

B. PURPOSE

With increasing reliance on data for decision-making and project implementation, it is essential to establish clear guidelines for data sharing to ensure that data is used ethically and in compliance with relevant laws and regulations.

The purpose of this Policy is threefold:

1. To safeguard personal, financial, and proprietary information from unauthorised access and breaches.
2. Promote Responsible Data Sharing: To enhance internal and external collaboration by providing clear guidelines for data sharing, ensuring data is shared in a controlled and secure manner.
3. Compliance: To comply with national and international data protection laws and regulations, including but not limited to the Digital Personal Data Protection (DPDP) Act and any other applicable legal frameworks.

C. ACKNOWLEDGEMENT

Each employee is required to sign a declaration form attached towards the end of this policy stating that:

1. S/he has read and understands the Data Sharing Policy
2. S/he will report to the Data Protection Officer/ line manager and/or project manager any suspected incident of data breach.

Policy non-compliance: Non-compliance with this policy may result in disciplinary action, including but not limited to termination of employment or contractual agreements.

D. SCOPE

This policy applies to all employees, contractors, consultants, and third-party partners of the Company who collect, access, handle, or share data as part of their role with the Company.

The policy covers all types of data, including but not limited to personal data, financial data, project data, and research data, in both digital and physical formats.

E. DEFINITIONS

1. Data

   Any information collected, processed, stored, or shared by the Company, including but not limited to text, images, videos, and databases.

2. Sensitive Data

   Data/Information that requires protection due to its confidential nature, such as personal information, financial records, proprietary information, and any data classified as sensitive under applicable laws and regulations.

3. Data Sharing Agreement (DSA)

   A formal document outlining the terms, conditions, and responsibilities of parties involved in sharing data externally.

4. Data Protection Officer (DPO)

   The individual responsible for overseeing data protection strategies and ensuring compliance with data protection laws and policies within the Company. The management of the company has designated Vice President, Mr. Ambuj Nayan as DPO (also refer (L) below).

F. PRINCIPLES OF DATA SHARING

1. Confidentiality: Data should be shared in a manner that protects sensitive information from unauthorized access, disclosure, or misuse. Measures should be in place to ensure that only authorized individuals have access to sensitive data.
2. Transparency: Data-sharing activities should be conducted transparently, with clear communication about the purpose of data sharing, how data will be used, and the measures in place to protect it. This includes providing stakeholders with information on data-sharing practices and obtaining necessary consent.
3. Accountability: Individuals and departments involved in data sharing are accountable for following established procedures and ensuring data protection. This includes documenting data-sharing activities and being responsible for any data they share.
4. Compliance: All data-sharing activities must comply with relevant laws, regulations, and organisational policies. This includes adhering to data protection laws, industry standards, and contractual obligations with external partners.

G. ROLES AND RESPONSIBILITIES

1. Managing Director

   As the custodian of the Data Sharing Policy, the Managing Director approves the Policy and its subsequent revisions.

2. Data Protection Officer (DPO)

   Data Protection Officer (DPO) has a primary responsibility for the implementation of this Policy throughout the Company. In addition, DPO is responsible for conducting investigations on report(s) of breaches.

   Also, DPO is responsible for providing guidance on data protection issues and ensure compliance with legal and regulatory requirements.

3. Human Resource (HR)

   Human Resource (HR) department is responsible for disseminating the Policy to all employees of the Company through internal communication channels. In addition, HR department shall ensure all Staff members understand the Policy and acknowledge the receipt.

   HR department will provide regular training to employees on data protection and sharing best practices.

4. Employees

   Adhere to the Data Sharing Policy and report any concerns or incidents related to data protection to DPO. Participate in training programs and follow established procedures for data sharing.

5. IT Department

The IT department is responsible for implementing technical measures to protect data, such as encryption and access controls. In addition, IT department supports data-sharing activities by providing secure platforms and tools.

H. DATA SHARING PROCEDURES

1. Internal Data Sharing

- Authorisation: Data should only be shared with individuals or departments that have a legitimate need to access it. Authorisation protocols should be established to verify and approve data-sharing requests.
- Access Controls: Implement role-based access controls to limit access to data based on job responsibilities and the principle of least privilege. Access permissions should be regularly reviewed and updated.
- Data Minimisation: Share only the minimum amount of data necessary for the intended purpose. This reduces the risk of data exposure and ensures that only relevant information is shared.

2. External Data Sharing

- Purpose and Use of Data: The service/ contract agreement with external parties must explicitly define the purpose for which the data is being shared and specify the intended use. This agreement must clearly state that any use of the data beyond the specified purposes requires prior written consent from the Company. This ensures that data is only used in ways that are authorized and beneficial to both parties, maintaining control and integrity of the shared data.
- Data Use, Protection, and Privacy Procedures: The service/ contract agreement must establish comprehensive procedures for the use, protection, and privacy of the data. This includes, but is not limited to, outlining the steps to be taken to ensure data is used in compliance with the agreed purposes, detailing the security measures to protect the data from unauthorised access, breaches, or misuse, and specifying the protocols to ensure data privacy is maintained. These procedures should be in accordance with applicable data protection laws and regulations and should include regular audits and updates to the security practices to address any emerging threats or vulnerabilities.
- Due Diligence: Conduct due diligence to assess the data protection measures of external partners. Ensure they have adequate safeguards in place to protect shared data and comply with relevant regulations.
- Data Anonymisation: Where feasible, anonymise data before sharing it externally to protect the privacy of individuals. Anonymisation techniques should be robust to prevent re-identification of individuals.

I. DATA PROTECTION MEASURES

1. Encryption: Use strong encryption methods to protect data during transmission and storage. Ensure that encryption keys are securely managed and regularly rotated.
2. Access Logs: Maintain comprehensive logs of data access and sharing activities. These logs should include details such as who accessed the data when it was accessed, and what data was shared.

J. DATA BREACH RESPONSE

1. Reporting: Employees should immediately report any incidents of suspected data breaches to the Data Protection Officer (refer L. Whom to Contact? for contact details of DPO).

   To the extent possible, the following details should be included in the report (report should be as specific as possible):

- The type of alleged breach
- Where and when the breach(es) occurred
- Who is involved and who else has the knowledge about the breach

Also, documentary proof(s) that is important for investigations should be included with the report or sent, at the earliest possible.

2. Investigation: The DPO will conduct a thorough investigation of reported data breaches. Identify the cause, assess the impact, and implement corrective actions to prevent future breaches.

   Once the investigations are complete, due & appropriate action which could include disciplinary action, civil or criminal action or closure of the matter if it is proved that breach is not committed, etc. shall be undertaken by the management of the Company.

3. Notification: Notify affected individuals and relevant authorities following legal requirements, as necessary. Notifications should include details of the breach, potential impacts, and steps taken to mitigate risks.

K. TRAINING

HR Department shall provide regular training to employees on data protection and share best practices. Training should cover topics such as data handling, recognizing and reporting data breaches, and compliance with data protection laws.

L. WHOM TO CONTACT?

For questions or concerns about the Data Sharing Policy, employees and partners can contact the Data Protection Officer (DPO) at:

Mr. Ambuj Nayan
Vice President
Mobile : +91 9871815469
Email : ambuj@gtechinfra.in

M. MONITORING AND REVIEW

This Policy will be monitored and reviewed for effectiveness and review the implementation of this Policy, on an annual basis.

The Company reserves the right to modify this Policy unilaterally at any time, without notice. Modifications may be necessary to maintain compliance with local regulations and/ or accommodate organisational changes in the company. Any revisions in this Policy including amendments or changes under respective clauses will be duly notified to employees through email communication. Also, such revised Policy or notification/ circular/ internal communication on such revisions will be updated on the Corporate Website (www.gtechinfra.in). The employee shall be deemed to have read, understood and acknowledged the changes thereof which will supersede the terms of the current Policy or any subsequent document/communication related to the Policy.

DECLARATION

I hereby declare that I have read and understood Data Sharing Policy and I hereby agree to abide by it.

Name :

Designation :

Signature :

Date :

Place :