TheRockGroup

Privacy & Data Protection Policy of TheRockGroup Holding B.V.

Last update: 31-10-2024
This documentation is subject to European GDPR and Dutch AVG law.

1. Identification of the Data Controller

Company Name: TheRockGroup Holding B.V.
Address: Mauritskade 64, 1092 AD Amsterdam, The Netherlands
Chamber of Commerce Number: NL 54707919

Data Protection Officer (DPO):
Name: Rixt van der Giessen
Email: rixt.van.der.giessen@therockgroup.biz

This policy outlines TheRockGroup's (TRG) commitment to protecting the privacy and rights of all individuals whose data we process, aligning with the requirements set by the General Data Protection Regulation (GDPR).

2. Scope of Data Processing Activities

TheRockGroup is a sustainability consultancy operating across three core domains:

1. Sustainability Strategy and Implementation
2. Sustainable Business Development
3. Education

As part of these services, TRG processes data solely as required for client projects and never engages in data processing unrelated to these purposes. Specific projects may include advisory services, sustainability reporting, and corporate compliance services.

Personal Data Processed:
TRG limits data processing to essential business contact information shared by clients, such as email addresses, and refrains from collecting sensitive personal data unless required and anonymized. All personal data remains strictly within the control of client-authorized platforms, and data sharing is restricted to the specific project scope.

3. Purpose of Data Processing

TRG processes limited personal data solely to:

- *Facilitate Communication and Project Execution*: Contacting client representatives and facilitating project deliverables.
- *Maintain Client Relationships*: Providing regular updates and ensuring high-quality service delivery.

Where TRG collects survey or project-related data, it remains anonymous and fully compliant with client systems, which generally provide the necessary security framework. If a client's systems do not provide the necessary security frameworks for handling survey or project-related data, TRG will implement several measures to ensure data security and GDPR compliance, such as Data Anonymization Techniques or a different, secure GDPR-compliant survey tool.

4. Data Access and Security

TheRockGroup implements data protection by design and by default, with a focus on preventing unauthorized access or misuse. Measures include:

- *Limited Access*: Access to data is restricted by employee role and project involvement.
- *Secure Infrastructure*: TRG uses OneDrive with data storage specifically configured for the EU, ensuring compliance with GDPR requirements.
- *Data Processing on Client-Secure Systems*: if a client provides TRG with a designated Client-Secure System and requires exclusive use of this system for project-related activities, TRG will ensure that all client data is processed solely within the provided Client-Secure System

Device and Data Security Measures:

- *Two-Factor Authentication (2FA):* All TRG accounts employ 2FA to secure access.
- *Password-Protected Devices and 1Password Management:* Passwords are securely managed, with restricted device access.

5. Data Retention and Disposal

TRG retains data only for the duration necessary to complete the project or as explicitly agreed upon with the client. All client documents are stored in designated folders labeled “Received from Client” or “Working Documents” to ensure transparency and easy retrieval. At the end of a project, TRG deletes or archives client data according to the established client agreement.

6. Incident and Data Breach Management

TRG follows a structured protocol for responding to data breaches. Our Data Protection Officer (DPO) and IT team actively monitor systems for suspicious activity, alerting management and initiating containment measures immediately in the event of a breach. Clients and relevant supervisory authorities are promptly notified in the case of a confirmed breach.

7. Technical and Organizational Security Measures

TRG has implemented various security measures to protect data, including:

- *Role-Based Access Control (RBAC):* Access permissions are granted based on project involvement and employee roles.
- *Access Revocation:* User access is promptly deactivated upon employee departure or project completion.
- *Regular Backups:* Data is regularly backed up to prevent loss, and stored securely on a local off-site server under management of IT Fix.

Additional technical safeguards include firewalls, anti-virus software, and spyware detection to prevent unauthorized access.

8. Third-Party Data Processors and International Transfers

TRG has offices in the Netherlands, Belgium, and South Africa. All data from TheRockGroup's projects is stored within the European Union by Microsoft, ensuring data protection compliance.

9. Employee Awareness and Training

To foster a culture of privacy and security, TRG provides regular training for employees, including:

- *Awareness Programs*: Instructional emails, training videos, and team sessions on GDPR practices.
- *Ongoing Training Sessions*: Online and in-person sessions to reinforce data protection practices and address updates in security requirements

10. Your Rights as a Data Subject

TRG is committed to upholding your rights under the GDPR. You have the right to:

- Access and Rectification: Request access to your personal data or make corrections.
- Erasure (Right to be Forgotten): Request deletion of your data where legally permissible.
- Restriction of Processing: Limit processing under certain conditions.
- Data Portability: Receive your data in a commonly used format or have it transmitted to another controller.
- Objection: Object to specific processing activities, based on a legitimate interest.

To exercise your rights or for any questions, contact our DPO at rixt.van.der.giessen@therockgroup.biz.