


Data Protection Policy

Version: 6

Issue date: January 2025

RCPO00020	Data Protection Policy
<p>ISSUE DATE December 2020</p> <p>REVIEW DATE January 2025</p> <p>NEXT REVIEW DATE January 2026</p> <p>VERSION 06</p>	<p>AUTHORISED BY:</p>  <p>Mark Taylor CEO</p>

Version Change Summary		
New Version ID	Date of Change	Summary of Changes
1	3/12/2020	Creation
2	26/01/2021	Revisions [CIO/Damm Solutions]
3	14/01/2022	No change - review
4	28/03/2023	Deleted reference to Sherwood House.
5	09/10/2023	Revised DPO
6	22/01/2025	Section 6 & 8 added data protection risk, breach. Updated CEO Details.

1. INTRODUCTION

Rock Compliance Ltd (“The Company”) needs to collect and use certain types of information about the people with whom it deals in order to operate the business in an effective and responsible manner. This information can include current, past and prospective employees, suppliers, clients/customers and others with whom it communicates. In addition, it may occasionally be required by law to collect and use certain types of information of this kind to comply with the requirements of Government departments for example, business data. There are safeguards within UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018 (DPA 2018), to ensure that personal information is dealt with properly, however it is collected, recorded, and used.

We regard the lawful and correct treatment of personal information by the Company as very important to successful operations and to maintaining confidence between those with whom we deal and ourselves. We must ensure that our organisation treats personal information lawfully and correctly.

To this end we fully endorse and must adhere to the ‘Principles’ set out in Article 5 of the UK GDPR. Specifically, the ‘Principles’ require that personal information:

- a) “Lawfulness, Fairness & Transparency”
Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.
- b) “Purpose Limitation”
Shall be collected for specified, explicit and legitimate purposes and not further processed in a

manner that is compatible with those purposes.

- c) "Data Minimisation"
Shall be adequate, relevant and where necessary, kept up to date.
- d) "Accuracy"
Shall be accurate and where necessary, kept up to date.
- e) "Storage Limitation"
Shall not be kept for longer than is necessary for that purpose or those purposes.
- f) "Integrity and confidentiality" –
Shall be processed in accordance with the rights of data subjects under the Act;
- g) "Accountability"
The controller shall be responsible for and be able to demonstrate compliance with the above.

2. DATA CONTROLLER

Rock Compliance is registered with the Information Commissioner's Office as a Data Controller, the Company is responsible for all the personal data they hold.

All outside communications, queries and subject access requests relating to Data Protection issues should be addressed to the Data Protection Officer to dpo@rockcompliance.co.uk.

3. DATA PROCESSING

It is the policy of the Company to aim to ensure that all relevant statutory requirements are complied with and that the Company's internal procedures are monitored periodically to ensure compliance.

It is the policy of the Company to endeavour to comply with any relevant Industry Codes of Practice issued by the Information Commissioner on the processing of data. In particular to endeavor to comply with the following conditions:

- a) Observe fully conditions regarding the fair collection and use of information
- b) Meet its legal obligations to specify the purposes for which information is used
- c) Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
- d) Ensure the quality of information used
- e) Apply strict checks to determine the length of time information is held
- f) Ensure that the rights of people about whom information is held can be fully exercised under the Act (these include; the right to be informed that processing is being undertaken; the right of access to one's personal information; the right to prevent processing in certain circumstances; the right to correct, rectify, block or erase information which is regarded as wrong information).
- g) Take appropriate technical and organisational security measures to safeguard personal information.
- h) Ensure that personal information is not transferred abroad without suitable safeguards.

In addition, The Company will ensure that:

- a) In accordance with the DPA 2018, subject access requests will be actioned within one calendar

month of the request being received. This time starts from receipt of identification from the data subject.

- b) In accordance with the DPA 2018 the company will charge £10.00 for subject access requests deemed repetitive or excessive by the Company.

Data Protection is a responsibility shared by employees of the Company and employees have a duty to adhere to the rules, procedures and instructions that may be used from time to time by the Company to ensure this policy is effective. Disciplinary action will be taken against any employee who fails to comply with these rules and procedures.

The Company will take such measures as may be necessary to ensure the proper training, supervision and instructions of all relevant employees in matters pertaining to Data Protection and to provide any necessary information.

Each line manager and supervisor will have immediate responsibility for data protection matters in his/her own area of work.

4. THIRD PARTY PROCESSING

The Company will pass any data collected to third parties that assist the Company in the operation of its business. The information will only be passed to organisations that fully comply with the DPA 2018 and so ensure the security, integrity and quality of the data as if it was held solely by the Company.

5. DATA SECURITY

Because we may hold sensitive data due to the nature of our business, all staff are responsible for ensuring that:

- Any personal data which they hold is kept secure
- Personal data is not disclosed

6. DATA PROTECTION RISK

This policy helps to protect Rock compliance from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should feel free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

7. RESPONSIBILITY

All employees within the scope of this policy are required to adhere to its terms and conditions.

Rock Compliance Board of Directors is responsible for communicating this Policy to Managers. Individual Managers are responsible for ensuring that this Policy is applied within their own area. Any queries on the application or interpretation of this Policy must be discussed with a nominated Director prior to any action being taken.

Rock Compliance Board of Directors has the responsibility for ensuring the maintenance, regular review and updating of this policy. Revisions, amendments, or alternations to the policy can only be implemented following consideration and approval by the nominated Director.

8. BREACH

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, Rock compliance shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO [more information on the ICO website](#)

9. REVIEW

This Policy will be reviewed periodically to ensure it reflects current legislative requirements and best practice. Any changes will be brought to the attention of all employees.