

1 The Controller - Who we are

- 1.1 MONTRACON LIMITED.

2 Data Protection

- 2.1 All members of the DPC have received training on data protection, Cyber Security and information security relating specifically to their responsibilities. In addition, at least one of the members of the DPC, will hold, or be working towards a General Data Protection Regulations Practitioner Certificate and at least one will hold, or be working towards a Certified Information Security Manager (CISM) Certificate.

- 2.2 The DPC can be contacted by emailing lucy.watkinson@Montracon.com or by writing to:

Data Protection
MONTRACON LIMITED Carr
Hill, Doncaster, DN4 8DE

3 Categories of Data Collected

- 3.1 Much of the information is provided by the employees themselves, but some may come from other internal sources, such as managers, or in some cases, external sources, such as referees. The information we hold includes, but is not limited to, application forms or CVs and references, proof of identity documents, right to work evidence, background checks, driving licences, verification of professional qualifications / memberships / certifications, contracts of employment and any amendments to it; correspondence with or about you our employees; information needed for payroll, benefits and expenses, including court judgements and attachment to earnings orders; pensions, insurance provisions, general contact details and emergency contact details; records of holiday, sickness and other absence; information needed for equal opportunities monitoring policy; and records relating to career history, such as training records, appraisals, other performance measures and, where appropriate, disciplinary and grievance records. Contact details, names, addresses, private email addresses are collected and retained for hard copy and or electronic communication purposes pertinent to legitimate business interests in communicating with our employees. Personal Data is protected in law by the General Data Protection Regulations (EU 2016/679), the General Data Protection Regulations (UK 2020), and The Data Protection Act (UK 2018)

4 Processing of Data

- 4.1 As an employer, and as a Group we may sometimes need to process personal data to pursue our legitimate business interests, for example to prevent fraud, administrative purposes or reporting potential crimes and process information about our employees for employment purposes. The information we hold and process will be used to enable us to manage our relationship with our employees effectively, lawfully, fairly and transparently, during recruitment, whilst they are working for us, at the time when their employment ends and after they have left our employment. This may also include using information to enable us to comply with their employment contract, to comply with any legal obligations, and protect our legal position in the defence of legal proceedings.
- 4.2 We will never process employees' personal data where these interests are overridden by their own statutory rights and freedoms. Where an employee chooses to not provide some or all of this data, we may be unable in some circumstances to comply with our obligations and we will tell them about the implications of that decision, if the situation arises.
- 4.3 Our employees will, of course, inevitably be referred to in many company documents and records that are produced by them and their colleagues in the course of carrying out their duties and the business of the company. All employees should refer to all the Data Protection Policies which are available on the Company SharePoint or in electronic format from lucy.watkinson@Montracon.com. All legal basis for processing personal data will meet the requirements of Article 6 of the General Data Protection Regulations.

5 Special Category Data

- 5.1 Where we process special categories of information relating to employees' racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, biometric data, health or sexual orientation, gender preferences and or identity we will always obtain their explicit consent to process this data unless this is not required by law or the information is required to prevent discrimination, or Preserve life in an emergency. Where necessary, we may keep information relating to our employees' health, which could include reasons for absence and GP reports and notes. This information will be used in order to comply with health and safety and occupational health obligations, to consider how health might affect ability to do a specific job and whether any reasonable adjustments to a job might be appropriate, in addition to providing evidence to the courts, when required. We will also need this data to administer and manage statutory and company sick pay, health insurance and or Death in Service policies.

6 Who will receive the data

- 6.1 We will only disclose information about our employees to third parties if we are legally obliged to do so or where we need to comply with our contractual duties, for instance we may need to pass on certain information to our payroll provider, pension or insurance schemes.
- 6.2 We may transfer information to other group companies for purposes connected with employment matters, or the management of the company's business.

- 6.3 If in the future we intend to process employee's, or groups of employees' personal data for a purpose other than that which it was collected we will provide them with information on that purpose and any other relevant information.

7 Payroll, Workplace Pension, Insurance and Benefit Providers

- 7.1 Where we are legally obliged, contracted to, or in the legitimate business interests of the company, we may need to provide employees' personal data to third party payroll, pension, insurance or benefit providers (for example for payroll processing, auto enrolment, and health or liability insurance). When we introduce employees to these providers, who are third parties, they form a direct and separate relationship with our employees, as their own members. In doing so they will become controllers of that personal data, in their own right. The providers will be able to issue those members with their own Terms and Conditions, alongside their own Privacy Notices and Data Protection Policies. These disclosures will fall within the reasonable expectations of an employee, employer relationship, where obligations of the employer's duties may be met by a third party. Rights and Freedoms of Individuals protected by the General Data Protection Regulations, will still apply.

8 International Transfer

- 8.1 MONTRACON LIMITED, on rare occasions may be legally obliged to provide some information to other countries within EEA, such as Republic of Ireland etc. for border/custom control, right to work, and inter-state taxation. If we are required to transfer data outside of the EEA, we will discuss those obligations with the relevant parties at that time. Some data may be processed on cloud based servers which have storage facilities outside the EEA, but the data is encrypted and protected by International Standard Contract Clauses and Treaties which prevent the data being accessed or further processed outside the EEA.

9 Retention Period

- 9.1 All personal data will be retained in accordance with our legal obligations and statutory minimum requirements.

10 Your Rights

- 10.1 MONTRACON LIMITED undertakes to protect the rights and freedoms of all individuals whose data we process. We will uphold the principles in Article 5 of the General Data Protection Regulations, and the rights provided under statute by any Act of the UK Government. We respect any individual's right to:
- Submit a Subject Access Request for their personal data (Article 15 GDPR)
 - Request correction and/or deletion of inaccurate or incorrect personal data (Article 16 GDPR)
 - Object to our processing of their personal data, if our processing is not lawful, fair, nor transparent (Article 18 GDPR)

- Have us explain to you the impact of failing to provide, withdrawing consent, or objecting to our processing of your personal data and the effects that may have (Article 13 GDPR)
- The right to request erasure of your data, if it has been collected in error, no longer needed, unnecessary, unlawfully processed, or obtained (Article 17).

10.2 If an individual is unhappy about the way the Data Protection Committee deal with their rights and freedoms, they can complain in writing to:

Chief Executive Officer
MONTRACON LIMITED Carr
Hill, Doncaster, DN4 8DE

10.3 The Chief Executive Officer or his nominated deputy will conduct an investigation and review of the circumstances and advise them of the findings along with any recommended actions within one month.

10.4 If the individual is still unsatisfied with the response of the Chief Executive Officer, or in fact at any other prior stage of the process, they can submit a report to the Information Commissioner's Office.

11 Automated Processing and Monitoring

11.1 We monitor internet, email, computer, telephone/mobile use, as detailed in our computer/telephone/electronic communications/expenses acceptable use policies, issued in addition to the contract of employment. We also keep records of employee hours of work by way of various Time Management Systems and or as detailed in the company handbook. We deploy GPS tracking of company assets. We keep tachographic data regarding journeys of relevant vehicles, in compliance with our legal obligations.

12 Biometric Data

12.1 CCTV is in use throughout various areas of Group properties, to detect and assist in the prosecution of crime, security of the company assets and defense of legal claims. Individuals present at any of our premises may be recorded by CCTV systems. Where this is taking place appropriate signage will be displayed.

Employee Privacy Notice

Document Control

Reference: DOC ISMS 0026

Issue No: 2.0

Issue Date: 02/04/2024

Page: 5 of 5

Document Control

The Data Protection Committee is the document owner and responsible for ensuring this policy remains current and up to date.

A current version of this document is available to all members of staff on the [Security and Governance SharePoint site](#) and is published by the Security and Governance function.

Change History Record

Issue	Description of Change	Date of Change
1.0	Initial Issue	
2.0	Review	02/04/2024