General Record of Processing and Data Protection Policy

1. Overview

Manor Resources is committed to handling data with the same care, integrity, and professionalism that underpins all our work. We believe that protecting the privacy and rights of individuals is core to the service we deliver for our clients.

This policy brings together all details of our data processing into one place, creating a single, reliable source of truth for training, administration, and decision-making within MR. Although we are a small organisation with fewer than 250 people, the nature of our work means we process both personal and Special Category (SC) data on behalf of clients to support their day-to-day employment obligations. For that reason, this policy also includes an Appropriate Policy Document (APD).

We ask all employees and sub-contractors to share responsibility for protecting data - our own and that of our clients - by following the guidance set out in this policy and other linked policies listed below.

Our data controller is Zoe Jones, zoe@manorresources.co.uk. Any issue or breach should be reported to Zoe in the first instance. This policy is supported by the following policies and documents:

- Data retention policy
- Use of IT policy
- Privacy Notice
- Ethical Marketing Policy (detail on marketing consents)
- Recruitment Policy (detail on automated decision making in recruitment)

Protecting personal information is not a one-time task; it is an ongoing commitment that requires awareness, consistency, and the willingness to adapt as risks and regulations evolve.

2. Purpose of Processing

We process SC data for employment on behalf of our clients. The MR's business activity data does not include Special Category data. We are data processors in our client's businesses, and these considerations have been made for that purpose.

3. Categories of data subjects collected

Employees
Job Applicants
Contractors
Consultants
Apprentices
Next of Kin

4. Categories of personal data collected

Basic personal identifiers
Economic and financial data
Identification data
Location data
Official documents

5. Categories of SC data collected

Health data
Sexual orientation data
Trade union membership
Religious or philosophical beliefs
Racial or ethnic origin

6. Recipients of the data

MR employees and sub-contractors
Line Managers (within client businesses)
Business owners (within client businesses)
Payroll providers (internal to client businesses or external contractors)
Administrators (within client businesses)

7. Appropriate Policy Document (APD)

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an APD to be in place when processing SC data. MR is documenting our APD in line with the requirement to process employment data on behalf of our clients.

This document demonstrates our compliant processing of SC data in line with the principles of Article 5 of the GDPR.

The purpose of completing this APD is to ensure that we, on behalf of our clients, undertake the highest level of protection and security when supporting clients with their employment activities.

Although an this APD outlines SC data, this outlines how Manor Resources processes all personal data, categories outlined in number 4 above.

Description of data processed
• Personal Data Basic personal identifiers Economic and financial data Identification data Location data Official documents • Special Category Data Racial or ethnic origin Religious or philosophical beliefs Trade union membership Health Sexual Orientation

Schedule 1: Condition for processing
Explicit Consent Employment, social security, and social protection Legal claims and Judicial acts Health or social care

Procedures for ensuring compliance with the principles
Accountability principle
By identifying the level of data that we process on behalf of our clients, we have chosen to document our data processing activities in line with the potential risk. As a small business with less than 250 employees, we consider that this documentation goes beyond what is required. By that nature, we are taking a 'by design and default' approach to data security. This document outlines what data we process on behalf of clients and who the data subjects may be. Any changes to this processing at MR will be outlined in this document. Our outsourced cyber security expert provides IT assistance to MR and inducts new staff in line with our data protection principles. Alongside this induction, we introduce new team members to the principals of the document at their first team meeting, which we hold weekly. We have contractual agreements for data sub-processors and induct them in 'constant diligence' regarding data protection. AI is a constantly evolving area and our commitment to ensuring the integrity of confidentiality with data can be found in our AI Policy. However, as a blanket rule, no personal data is permitted to be entered into any open-source AI platform. We have a running agenda item at quarterly team meetings for data considerations to ensure that improvements are front of mind when working with clients. Information about how and why MR processes data can be found in our Privacy Policy; however, this does not include how and why we process the information on behalf of our clients. That information is all contained within this document and should be considered to be processed for an obvious purpose – employment.
Principle (a): lawfulness, fairness and transparency
The lawful basis for processing can be found in this document, with an outline of all data collected at any time. This document is regularly reviewed to ensure it is kept up to date. Information on version control is kept on file so we can learn from the improvements we make.

We outline (on our data collection strategies, such as forms) the purpose of collecting each piece of data and only collect required information, not 'nice to have' or 'just in case' data.

We are constantly improving systems and processes to ensure that specific data is only accessed by individuals within the business who need to use it, i.e. economic and financial data accessed by payroll administrators and not line managers or next of kin information accessed by Line Managers, not payroll administrators.

We use available technology to aid us in limiting data sharing in this way.

Information about how and why MR processes data can be found in our Privacy Policy; however, this does not include how and why we process the information on behalf of our clients. That information is all contained within this document and should be considered to be processed for an obvious purpose – employment.

Clients are exposed to how we will process data on behalf of their employees in their contracts, and we include this documentation with their onboarding.

Principle (b): purpose limitation

The purpose for our processing can be found in this document, with an outline of any and all data we may have at any time collected. This document is regularly reviewed to ensure it is kept up to date. Information on version control is kept on file so we can learn from the improvements we make.

If we use need to use personal data for a new purpose (other than a legal obligation or function set out in law), we check that this is compatible with our original purpose and will get specific consent for the new purpose.

Principle (c): data minimisation

We process data on behalf of our clients and use our knowledge, understanding and 'by design and default' approach to data collection to advise what and how they collect data. Ultimately, the choice of what data they collect is the client's choice.

We carry out regular and extensive data processing training within MR to ensure we can support them to comply with their employment processing.

We use all system and process improvements when updating employee onboarding processes as an opportunity to ensure that data collection is minimised to the essential data categories.

We recommend and support clients to retain data in line with the following CIPD suggestions - here.

As a business, we retain emails and associated documentation related to the client's status as a client of MR indefinitely to support us in winning new business.

AI is a constantly evolving area and our commitment to ensuring the integrity of confidentiality with data can be found in our AI Policy. However, as a blanket rule, no personal data is permitted to be entered into any open-source AI platform.

Regarding data held on the client's employees, we delete that in line with the above CIPD suggestions.

Principle (d): Accuracy

When we start working with a client, we audit the documentation they have in place and what data they hold on their employees to ensure its accuracy.

This is to ensure compliance with staff safety (i.e., Next of Kin data is kept on file and up to date) and legal compliance (i.e., Right to Work in the UK data has been collected).

We support clients to increase the accuracy of obtaining data by improving their data collection strategies, for example, by collecting information online.

As part of our annual data clean-up activities, we support clients in reviewing, amending, and recording data errors and adapting systems to ensure repeat mistakes are not made.

Principle (e): Storage limitation

We recommend and support clients to retain data in line with the following CIPD suggestions - here.

As a business, we retain emails and associated documentation related to the client's status as a client of MR indefinitely to support us in business development.

In line with the information below, we conduct an annual review with our clients of the data we hold and keep/delete as per the CIPD guidelines.

Principle (f): Integrity and confidentiality (security)

We use Office 365 tools to keep data sharing outside of the MR online area to a minimum, including keeping data sharing on email to a minimum.

We do not use recording equipment for phone calls to ensure that no information is unintentionally retained when spoken about verbally, as often can be the case with employee relations issues.

We actively support our clients to use online HR systems to capture and record data and ensure it is kept behind appropriate password-protected systems. We also support their use of online data-capturing tools (such as forms on Office 365) to minimise the need to record data in paper form.

If necessary, we send sensitive PDFs encrypted, and password protected and have a process to follow regarding revealing the password to the recipient.

It is always a work in progress, and we continuously learn and improve as we find new and innovative ways to share protected data.

Our outsourced cyber security expert provides IT assistance to MR and inducts new staff in line with our data protection principles.

Sub-contractors who are processing client data for Manor Resources Ltd do so using MR IT equipment so we can ensure that the hardware is set up according to our requirements to minimise risk.

All sub-contractors enter into data agreements with us upon onboarding which outline each of our roles in terms or controlling and processing data.

Retainer clients are instructed to set up a specific email address for MR consultants to use so that we can ensure that data transferred by email is kept within their business. This business-specific email access also gives access to clients' storage systems and means that file transfer outside of domains can be minimised.

We have clear roles outlined in our agreements with clients which outline each of our roles in terms of controlling and processing data.

AI is a constantly evolving area and our commitment to ensuring the integrity of confidentiality with data can be found in our AI Policy. However, as a blanket rule, no personal data is permitted to be entered into any open-source AI platform.

Retention and erasure policies
Annual reviews – December Using the CIPD suggestions here we: • Advise and support clients to check and update their employee data • Support clients to record where data is incorrect using our template • Advise and support clients to delete relevant data in line with CIPD requirements • Delete any client's employee data in line with CIPD requirements we have on our own systems. Basic personal identifiers – 6 years Economic and financial data – 6 years Identification data – 6 years Location data – 6 years Official documents – 6 years Health data – 6 years Sexual orientation data – 6 years Trade union membership – 6 years Religious or philosophical beliefs – 6 years Racial or ethnic origin – 6 years

APD review date
August 2025
Version number: 1.3

8. Data Protection Impact Assessment (DPIA)

We have considered the requirement for a DPIA on the premise that we process SC data and concluded that it is unnecessary for the predominant nature of the work at MR.

We undertake regular training sessions with our team and assess data considerations with DPIAs in mind. We have undertaken a specific team session on DPIA on 28th April 2025.

We review the need for a DPIA at our regular data processing reviews alongside the start of any major project involving the use of personal data.

- We consider whether to do a DPIA if we plan to carry out any:

- Evaluation or scoring.
- Automated decision-making with significant effects.
- Systematic monitoring.
- Processing of sensitive data or data of a highly personal nature.
- Processing on a large scale.
- Processing of data concerning vulnerable data subjects.
- Innovative technological or organisational solutions.
- Processing that involves preventing data subjects from exercising a right or using a service or contract.

- We always carry out a DPIA if we plan to:

- Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
- Process special-category data or criminal-offence data on a large scale.
- Systematically monitor a publicly accessible place on a large scale.
- Use innovative technology in combination with any of the criteria in the European guidelines.
- Use profiling, automated decision-making or special category data to help decide on someone's access to a service, opportunity, or benefit.
- Carry out profiling on a large scale.
- Process biometric or genetic data with any criteria in the European guidelines.
- Combine, compare or match data from multiple sources.
- Process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines.
- Process personal data in a way that involves tracking individuals' online or offline location or behaviour in combination with any of the criteria in the European guidelines.
- Process children's personal data for marketing purposes or offer online services directly to them.
- Process personal data that could result in a risk of physical harm in a security breach.

We carry out a new DPIA if there is a change to the nature, scope, context, or purposes of our processing.

If we decide not to carry out a DPIA, we will document our reasons and update this document as required.

9. Review and feedback

We continue to explore the different ways that we can ensure that data is kept secure during processing and consider it an essential part of our day-to-day work.

If you ever spot something in the way that we are handling data - or have suggestions for areas where we can improve - please let us know.

We value honest conversations and continuous improvement above all.