Data Protection Policy

Document Control:

Document filename	Data Protection Policy		
Director Lead	Jon Russell	**Status**	Live
Owner	Jon Russell	**Version**	V03
Author	Christopher Pratt	**Version Date**	June 2026
Retention period	Review Annually	**Configuration control**	No
Confidentiality	Private	**Distribution**	Moorhouse Consulting/ Customer

16th Floor, Dashwood House, 69 Old Broad St, London EC2M 1QS
+44 (0)20 3004 4482

Version Control:

Version	Date	Notes	Completed by
V01	October 2022	Initial Version	Christopher Pratt
V02	September 2025	Moorhouse template refresh and Minor updates	Christopher Pratt
V03	June 2026	Annual review no update	Ethan Box

Other Related Documents

Employee and Associate Privacy Policy
Data Retention Policy
Information Security Manual
Information Security Policy

Document Validation/Owner Interval: The document owner shall validate this document annually during the anniversary of the month of issue.

The document owner is Jon Russell, The Information Security Director, while the Information Security Director retains responsibility for approving the document the annual review and update may be delegated to the Information Security Manager.

Table of Contents

1. Introduction

Moorhouse is committed to the right to privacy for all individuals, including employees and clients, and the correct and lawful treatment of Personal Data. Moorhouse is committed to collecting, maintaining, securing, disclosing and using Personal Data in accordance with applicable laws, rules and regulations in force at any time and will only process data in accordance with the law.

The purpose of this Policy is to ensure compliance with regards to European Data Protection Legislation which covers: (i) the General Data Protection Regulation, ("GDPR"); (ii) the Data Protection Act 2018; and (iii) any other applicable law, rules and regulations in force from time to time ("European Data Protection Legislation").

This policy applies to all employees and officers of Moorhouse ("Employees"), and to temporary workers, consultants, contractors, agents and subsidiaries acting for, or on behalf of, the Company ("Associated Persons").

Any violation of this policy is likely to constitute a serious disciplinary or contractual matter for the individual concerned.

It is every Employee and Associated Person's responsibility to report any concerns regarding the treatment of Personal Data, about yourselves or others, to a Partner as soon as it is discovered.

This policy should be read in conjunction with the following documents:

- Data Protection Statement
- Employee Privacy Notice
- Applicant Privacy Policy
- Photograph and Filming Consent
- Information Security Policy
- Reporting Incidents Guide

2. Responsibility for compliance with Data Protection Legislation

Each Employee and Associated Person shall be responsible for complying with the European Data Protection Legislation by reference to this Policy and any related policies referenced herein.

3. Data Protection Legislation

The General Data Protection Regulation (GDPR) forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018). The main principles of this legislation is as follows:

- The GDPR applies to 'controllers' and 'processors'.
- A controller determines the purposes and means of processing personal data.
- A processor is responsible for processing personal data on behalf of a controller.
- Controller and processors have specific legal obligations for which there are legal sanctions if they are not complied with

Personal Data is information that relates to an identified or identifiable individual (natural person). Even if an individual is identified or identifiable, directly or indirectly, from the data, it is not personal data unless it 'relates to' the individual.
Personal data may also include Special Categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and only permitted to be processed in specific circumstances. See Appendix A.

4. Guiding Principles

Moorhouse will comply with the spirit of the key principles of GDPR:

a) **Lawfulness, fairness and transparency** – process personal data lawfully, fairly and in a transparent manner in relation to individuals;
b) **Purpose limitation** – collect personal data for specified, explicit and legitimate purposes and not further process in a manner that is incompatible with those purposes;
c) **Data minimisation** – personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
d) **Accuracy** - personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay;
e) **Storage limitation** - personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
f) **Integrity and confidentiality** – personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;
g) **Accountability** – demonstrate compliance with the key principles.

5. Lawfulness, fairness and transparency

Moorhouse has identified an appropriate lawful basis (or bases) for the processing of the following categories of personal data:

- Employees
- Applicants
- Clients
- Visitors to the Moorhouse website

Moorhouse will only process Special Categories of data or criminal offence data when it has a lawful basis upon which to do so.
Moorhouse will consider how the processing of personal data may affect the individuals concerned and will mitigate any adverse impact.
Moorhouse will only handle people's data in a transparent and fair manner. Moorhouse will not deceive or mislead people when we collect their personal data.

6. Purpose Limitation

Moorhouse has identified the purposes for processing the following categories of personal data:

- Employees
- Applicants
- Clients
- Visitors to the Moorhouse website

Moorhouse has documented these purposes and included details of these purposes in our privacy information for each category of personal data.
Moorhouse will regularly review our processing and, where necessary, update our documentation and our privacy information for individuals.

7. Data Minimisation

Moorhouse will only collect personal data required for a given processing purposes. However, Moorhouse will ensure it has sufficient personal data to properly fulfil those purposes.
Moorhouse will periodically review the data and delete anything we don't need, as set out in the relevant privacy notice.

8. Accuracy

Moorhouse will undertake all reasonable endeavors to ensure the accuracy of the personal data it holds.
Moorhouse will have appropriate processes in place to check the accuracy of the data we collect and where practical, record the source of that data.
Moorhouse will have processes in place to maintain records where necessary.

9. Storage Limitation

Moorhouse will ensure it adheres to relevant retention periods
Moorhouse will regularly review information and erase or anonymise personal data where practical and where it is no longer needed.
The Moorhouse retention periods are detailed in the relevant privacy notices.

10. Integrity and Confidentiality (Security)

The security measures that Moorhouse has in place to protect personal data are covered by the Information Security Policy.

11. Accountability

Moorhouse will put in place appropriate technical and organisational measures to meet the requirements of accountability including:

- adopting and implementing relevant data protection policies;
- ensuring contractual mechanisms are in place with organisations that process Moorhouse personal data;
- where required, maintain documentation of our processing activities;
- implementing appropriate security measures;
- record all data incidents
- report all data violations within 72 hours tothe relevant authority and individuals concerned

- ensuring Data Processing Agreements are in place with all clients.

12. Lawful Basis

Moorhouse must have a valid lawful basis in order to process personal data. Which basis is most appropriate to use will depend on the purpose or processing, the type of personal data and the relationship with the individual.

Moorhouse will determine the lawful basis before it begins processing. The lawful basis will be documented where required.

Moorhouse will include information about both the purposes of the processing and the lawful basis for the processing in the relevant privacy notice.

There are six available lawful bases for processing:

a) **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose.

b) **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c) **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).

d) **Vital interests**: the processing is necessary to protect someone's life.

e) **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

13. Individual Rights

Data Subjects have a number of rights under the GDPR which are as follows:

a) Right to be **Informed**: Moorhouse will provide privacy information to individuals at the time we collect their personal data from them (**Privacy Notice**).

b) Right of **Access**: Moorhouse will have processes in place to ensure that Moorhouse can respond to a **subject access request** within permitted timescales.

c) Right to **Rectification**: Moorhouse will have processes in place for individuals to have inaccurate personal data rectified, or completed if it is incomplete.

d) Right to **Erasure**: Moorhouse will have processes in place to ensure that Moorhouse can respond to a request for erasure within permitted timescales.

e) Right to **Restrict Processing**: Moorhouse will have processes in place to ensure that Moorhouse can respond to a request for restriction within permitted timescales.

f) Right to **Data Portability**: at the annual update of this policy this right is not considered relevant to Moorhouse.

14. Contracts

Whenever a controller uses a processor there must be a written contract in place so that both parties understand their responsibilities and liabilities.

Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply.

Where Moorhouse is acting as a Controller it will ensure that all contracts set out:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.
- Where Moorhouse is acting as a Controller it will ensure that all contracts include the following terms requiring the Processor to:
- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data violations and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract;
- submit to audits and inspections;
- provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations;
- tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

Client Contracts

Providing a service to a client does not mean that Moorhouse becomes its data processor in every case. Depending on the circumstances, the client will not have sole data controller responsibility even though they initiated the work by asking for advice. Responsibility also lies with Moorhouse because it determines what information to obtain and process in order to do the work and because it is answerable itself for the content. This would be a **Co- Controller** relationship.
The client is responsible for establishing the nature of the relationship with Moorhouse (and Moorhouse should satisfy itself) as one of:

A. Co-Controller – both the client and Moorhouse are Controllers (see above)

B. Processor – Moorhouse is processing data on behalf of the client

There is a third type of relationship known as Joint Controller where both parties are Controllers together. This is not a likely scenario but may include working with SQS and other group entities.

Framework contracts and Master Services Agreements will need to incorporate provisions for both Controller and Processor scenarios and use each work order to specify the detail such as any processing instructions.
Where Moorhouse is a Co-Controller, there must be a Data Sharing Agreement between both parties.
Where Moorhouse is a Processor, there must be a Data Processing Agreement for each engagement (the Services) that instructs Moorhouse as to what data is being made available, what can be done with the data during the Services and what should be done with the data at the end of the Services. There must also be a Data Processing Agreement for the data that Moorhouse provides to the client.

15. Data Protection by design and default

Moorhouse will promote privacy and data protection compliance in all projects and operations it undertakes and shall implement appropriate technical and organisational measures to comply with GDPR legislation. Moorhouse will:

- consider data protection issues as part of the design and implementation of systems, services, products and business practices.
- Where reasonably possible, make data protection an essential component of the core functionality of our processing systems and services.
- Undertake our best endeavours to anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.
- Where reasonably practical and possible, ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.

Moorhouse will complete a Data Protection Impact Assessment (DPIA) for processing that is likely to result in a high risk to individuals. There is a screening checklist available on the ICO website to help you decide when to do a DPIA.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation- gdpr/accountability-and-governance/data-protection-impact-assessments/

16. Personal Data Incidents and Violations

The GDPR introduces a duty on all organisations to report certain types of personal data violation to the relevant supervisory authority. Moorhouse will do this within 72 hours of becoming aware of the violation. If the violation is likely to result in a high risk of adversely affecting individuals' rights and freedoms, Moorhouse will also inform those individuals without undue delay.

Escalation Process

A data incident will not necessarily constitute a personal data violation. However, every data incident must be escalated as follows to determine whether a violation has occurred:

- **Client Data**: You must report any security incident regarding actual or suspected Personal Data violations of client data to the relevant Engagement Partner as soon as they are discovered
- **Moorhouse Data**: You must report any actual or suspected Personal Data violations of Moorhouse data to the Finance Director as soon as they are discovered.

A personal data violation can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

There will be a personal data violation whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed. Personal data violations can include:

- access by an unauthorised third party;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen; and
- alteration of personal data without permission.

When a personal data incident is reported a Moorhouse Partner will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then the Partner will notify the ICO; if it's unlikely then it will be recorded as an incident.

The notification to the ICO must include:

- the number and categories of individuals concerned;
- the number and categories of personal data records concerned;
- a description of the likely consequences of the violation;
- a description of the measures taken to deal with the violation and mitigating actions.
- https://ico.org.uk/for-organisations/report-a-violation/

All incidents must be recorded regardless of whether or not they need to be reported to the ICO. The incident report must detail the justification for not reporting the incident to the ICO.

17. Data Protection Officer

Moorhouse is not required to appoint a Data Protection Officer at the time of this policy as it does not reach the statutory threshold of 250 employees.

18. Information Commissioner's Office

Moorhouse will put in place appropriate technical and organisational measures to meet the requirements of accountability including
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

18. Policy Enforcement

Violation of this policy may result in your access to Moorhouse ICT systems using your corporate device and any personal devices being revoked. It may also lead to disciplinary action being taken against you in accordance with the company's disciplinary policies.

MOORHOUSE
AN EXPLEO COMPANY

16th Floor, Dashwood House, 69 Old Broad St, London EC2M 1QS
+44 (0)20 3004 4482

Appendix A: Special Categories of Personal Data

In order to process special category data there is an additional requirement to satisfy a specific condition under Article 9. This is because special category data is more sensitive, and so needs more protection. For example, information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

The conditions for processing special category data are listed in Article 9(2) of the GDPR:

a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;

b. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;

c. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body;

e. processing relates to personal data which are manifestly made public by the data subject;

f. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g. processing is necessary for reasons of substantial public interest;

h. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;

i. processing is necessary for reasons of public interest in the area of public health;

j. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes.

These conditions should be considered alongside the Data Protection Act 2018, which adds more specific conditions and safeguards.