

Document Name	Data Protection Policy
Document Reference	OMG – POL - 008
Document Issue Number	4
Document Review Date	January 2023

This policy and other documents referred to in it sets out the basis on which we will process any personal data that we collect from data subjects, or that is provided to us by data subjects or other sources. This policy does not form part of any employee’s contract of employment and may be amended at any time.

Omega is aware of its obligations under the General Data Protection Regulation (GDPR) and domestic data protection legislation, and is committed to processing your data securely and transparently. This privacy notice sets out, in line with current data protection obligations, the types of data that we hold on. It also sets out how we use that information, how long we keep it for and other relevant information about your data.

For the purpose of this policy the company is a “data controller”. The GDPR also gives individuals rights regarding their personal data including:

- The right to be informed
- The right to correction
- The right to access
- The right to object
- The right to restrict processing
- The right to erasure
- The right to data portability
- Rights regarding automation

In order to manage our business, we keep records about our employees that include the following. Please note this list is not exhaustive and can be changed:

- Full name
- Gender
- Date of birth
- Address
- Emergency contact information
- CV
- References
- Appraisals
- Qualifications
- CV’s
- Bank details
- Right to work information
- Criminal record checks (where necessary)
- Sickness record
- Health information
- Disciplinary record
- Proof of employment i.e. service agreement

We will process data about our staff and clients for legal reasons, because we have a legitimate business interest to do so or for the performance of a contract. Data will be shared with 3rd parties for the purpose of employment and/or contracts. These 3rd parties such as, but not limited to payroll companies, financial Institutions and governing bodies. Under GDPR some data is referred to as sensitive personal data and this refers to data such as the following:

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Health data
- Sexual orientation
- Criminal conviction data

We may process sensitive personal data relating to staff including, as appropriate:

- Information about any employee’s physical or mental health or condition in order to monitor sick leave and take decisions as to the employee’s fitness to work.

We need explicit consent from an employee in order to process their sensitive data, and if consent is given it can be withdrawn easily.

Our obligations

The six principles for processing personal data under GDPR are:

- Personal data should be processed fairly, lawfully and in a transparent manner
- Data should be obtained for specific and lawful purposes and not further processed in a matter incompatible with those purposes
- The data should be adequate, relevant and not excessive
- The data should be accurate and where necessary kept up to date
- Data should not be kept for longer than necessary
- Data should be kept secure

We are committed to following these principles and we ensure that all processing of data of which you are the subject is lawful. We will process data about you only as far as is necessary for the purpose of managing our business. Data will not be disclosed to anyone else other than our authorised employees, agents, contractors or advisors (except as required by law) unless you expressly authorise its disclosure. We will only obtain data about you that we require for the purpose of managing our business and dealing with you as an employee of that business.

We will take all reasonable steps to ensure that the data we process is accurate. Data will be retained as necessary during the course of your employment and we will follow all statutory retention periods. We will process data in accordance with your rights under GDPR.

Data will be kept in a secure system whether manual or computerised to the best of our ability at all times.

We will not disclose your data to a third party without your consent unless we are satisfied that they are legally entitled to the information. If your data is disclosed to a third party, we will ensure it still follows the six GDPR principles.

Our policy on access to data

- We have appointed a data protection officer
- On receipt of a request we will provide all data that we are obliged to disclose within 30 days of receipt of your request being received
- Should you wish to bring any inaccuracy in disclosed data to our attention, you are required to do so in writing
- We will ensure that all data is as accurate as possible and all necessary steps to ensure that this is the case and to rectify any inaccuracies will be taken.

Where we have requested a reference in confidence from a referee and that reference has been given on terms that it is confidential and that the person giving it wishes that it should not be disclosed to you, it is our policy that it is unreasonable to disclose the reference to you, unless consent is obtained from the person who gave the reference.

Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Protection Team at:

Maxine Myburg – Data Protection Officer – m.myburg@omegapersonnel.co.uk

A handwritten signature in black ink, appearing to read "Abdul Mukith".

Abdul Mukith – Managing Director