Mabe Allen LLP
Data Protection Policy

This is a statement of the data protection policy adopted by Mabe Allen LLP.

Definitions:

- A 'controller' determines the purposes and means of processing personal data.
- A processor is responsible for processing personal data on behalf of a controller.
- Client data refers to all data relating to the client and his employees (for payroll processing only) within the scope of the engagement letter.
- Employee data refers to all data relating to the employee.

Scope of Policy

We are required to collect and use certain types of personal information about the people we deal with:

- Employees (current, past and prospective).
- Clients (current, past and prospective).
- Suppliers.
- Others with whom we communicate with.

The data can be held in a variety of forms – digitally/electronically or hard copy.

In addition, we may occasionally be required, either by law or to carry out our responsibilities to collect, use and share certain types of personal information to comply with the requirements of Government departments, professional bodies, agencies and regulators.

Under the Data Protection Legislation, all organisations which handle personal information must comply with a number of important principles regarding the privacy and disclosure of this information.

We believe that the lawful and correct treatment of personal information is critical to our successful operation and to maintaining our stakeholders' confidence in us. We recognise that, to maintain our reputation and integrity as an open and professional organisation, we must be fully compliant with this legislation.

The Policy will be reviewed on an annual basis and updated in line with current legislation.

Data Protection Legislation

In the United Kingdom and the European Economic Area (EEA), "Data Protection Legislation" means all applicable data protection and privacy legislation or regulations including The Privacy and Electronic Communications (EC Directive) Regulations 2003 (also known as PECR) and any guidance or codes of practice issued by the European Data Protection Board or the Information Commissioner, together with:

- UK Data Protection Act 2018.

- From 25 May 2018 onwards Regulation (EU) 2016/679 (the "General Data Protection Regulation" or "GDPR"), as amended by the UK Data Protection Act 2018.

  Outside of the EEA, "Data Protection Legislation" means local, territorial data protection and privacy legislation that governs the processing of Personal Data.
- Money Laundering Regulations.
- Child Protection and Safeguarding Regulations.

Mabe Allen LLP's Responsibilities

We fully endorse and adhere to the principles of data protection set out in the Data Protection legislation and will:

- fully observe the conditions regarding the fair collection and use of personal information
- meet our legal obligations to specify the purposes for which we use personal information
- only collect and process the personal information needed to carry out our business or to comply with any legal/statutory requirements and regulations.
- ensure that the personal information we use is as accurate as possible
- ensure that we don't hold personal information any longer than is necessary
- ensure that people know about their rights to see the personal information we hold about them
- take appropriate technical and organisational security measures to safeguard personal information; and
- ensure that personal information is not transferred abroad without suitable safeguards.

In addition, we will ensure that:

- we will identify a person with specific responsibility for data protection in the organisation.
- we regularly review and audit how we handle personal information
- the ways we handle personal information are clearly described
- everyone handling personal information understands that they are responsible for following good practice
- everyone handling personal information is appropriately trained and properly supervised
- we regularly assess the performance of people who handle personal information
- anybody wanting to make enquiries about handling personal information knows what to do; and
- queries about handling personal information are deal with promptly and courteously
- we will ensure the security of electronic communication by way of encryption of data and control of portable IT equipment.
- we will never sell your details to someone else. Whenever we share your personal information, we will do so in line with our obligations to keep your information safe.
- We will ensure that any changes to existing procedures or the introduction of new procedures) met the standards set under GDPR by carrying out a data protection impact assessment to ascertain that is no risk to the rights and freedoms of individuals.

Data Protection Officer

The firm's Data Protection Officer is identified as Kevin Slack, Managing Partner, to whom all matters appertaining to Data Protection should be addressed at Mabe Allen LLP, 50 Osmaston Road, Derby, DE1 2HU.

Use of Personal Data

The firm will obtain and use personal data in the following ways:-

Employees (current, past and prospective)

- Personnel records
- Accident records
- Salaries including PAYE and NI
- Pension scheme
- Life Assurance scheme
- CPD Training Records

Clients (current, past and prospective)

- Within the scope of the agreed engagement letter
- As agents for processing client employee payroll
- Communications with statutory bodies and Government departments
- Referrals within the scope of the agreed engagement letter
- Use of credit card details for payments (in accordance with our Payment Card Industry Security Standard PCI DSS Policy).
- For 'Know Your Client' and money laundering checks.

Suppliers

- Identification details
- Proof of right-to-work
- Modern slavery

Others with whom we Communicate

- Unsolicited correspondence/emails (for example: CVs)

Visitors to our Premises/General Public via CCTV

- The firm obtains photographic data of visitors to the premises and/or the general public by use of CCTV for security purposes.
- The data records for one month and then over-writes. The data is therefore kept for one month only. No back-up copies are produced.
- The recorded data is not processed or shared with third parties unless requested by Police Officers/Authorities.
- The firm displays a sign at the premises where CCTV is in operation.

Supplier Compliance

The firm will ensure that suppliers who have access, through our IT systems, to personal data are fully GDPR compliant. We will do this by obtaining written confirmation from the supplier upon engagement.

Encryption of Data

- All of the firm's IT systems are password protected.
- Information held on USB devices should be encrypted.
- Emails containing sensitive information should be encrypted, wherever possible and where the recipient supports encryption.
- No personal information will be stored on portable hardware.
- No client information will be stored on employee personal devices or email accounts.

Destruction of Data

Digital/Electronic Data

- Client and employee records are securely held, in a locked cabinet, for the statutory period and then deleted from the network.
- Emails are deleted from individual Outlook accounts after the statutory period.
- The firm will ensure the secure destruction of all defunct IT equipment via specialist contractors and a Certificate of Destruction will be obtained and retained.

Hard Copy

The firm has a Shred-All Policy which requires the use of confidential, locked waste containers for all waste hard copy information and this is disposed of by a confidential waste contractor who issue a Certificate of Destruction and are GDPR compliant (see section 10 – Supplier/Contractor Compliance). Client and employee records are securely held for the statutory period and then destroyed using the above method.

Privacy Notices

These will be issued to all clients (upon engagement and available on the Firm's website) and to employees.

Implementation of new procedures/practices

When new procedures, practices or equipment are introduced, The Firm will carry out a an assessment to ascertain whether this will impact on personal data held by the Firm. There are two documents to assist in this process:

- Data Protection Impact Assessment Procedure
- Data Protection Impact Assessment

Training

The firm recognises the importance of ensuring all staff are fully informed and are aware of the implications of a breach. In order to do this all staff:-

- Will receive training regarding this policy and the GDPR legislation.
- Instructions will be given regarding the protocols for off-site visits.
- Up to date information will be circulated to all staff as appropriate.

Off Site Visits

During the course of their duties, staff may be required to carry out visits to client premises. Instructions will be given regarding the information that can be taken off site and the method for recording the data.

All staff should be aware that no equipment or client information files should be left in motor vehicles at any time or left unattended at client premises.

Should it be necessary for an employee to hold data overnight, this should be kept in a secure environment which is inaccessible to non-company staff.

Working from Home

It is possible for certain staff to access the Firm's network from home if, for specific reasons, they are unable to travel to company premises (sickness absence etc.).

In this case the same procedures in place for off-site client visits should be observed regarding the security of client data.

The Individual's Rights

- To be informed of the data to be processed in a clear, transparent and concise format
- To have access to your personal information.
- To have inaccuracies corrected.
- To have information erased (right to be forgotten).
- To restrict processing.
- To prevent automated decision making and profiling.
- Data portability – allows individuals to obtain and reuse their personal data for their own purposes across different services electronically.
- To object – processing based on legitimate interests or the performance of a task in the public interest, direct marketing or processing for scientific/historical research and statistics.

Dealing with Personal Data Breaches

The Firm has a procedure for dealing with any data breaches and this will include notifying the Information Commissioner's Office. If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the data breach, notification to these individuals will be carried out in a coordinated manner with the support of the DPO. The following documents support this:

- Data Breach Procedures
- Data Breach Notification Form
- Data Breach Evidence log
- Data Breach Management Flow Chart

Obtaining Data

The Firm has a procedure for any requests for copies of the personal information that we hold should be directed to Kevin Slack, Managing Partner, Mabe Allen LLP, 50 Osmaston Road, Derby, DE1 2HU. The following documents support this:

- Procedures for responding to Subject Access Requests
- Subject Access Request Form

Full information regarding this policy and the documents required for compliance can be found at:

www.mabeallen.co.uk/GDPR