G. Moore & Co. Ltd - Our policy towards Data Protection

It is our policy to treat customers, staff and all other stakeholders within the business (data subjects) fairly and lawfully when processing, storing and sharing their personal data.

We are registered with the Information Commissioners Office (ICO). Our registration number is ZA162731. Our registration is renewable every year on 17th December. Details can be viewed at https://ico.org.uk/esdwebpages/search

In addition we are required to ensure that our registration details remain up to date and any change is notified to the Information Commissioner's Office within 28 days of any change occurring.

Our firm will treat all personal information as private and confidential, even when the data subject's policies have lapsed or are cancelled or they are no longer employed by our firm; we will not release information to anyone else except where:

- The data subject gives us explicit, unambiguous consent
- Required under our authorisation by the FCA
- We have to by law
- Processing by another party, such as an insurer, is necessary for the performance of a contract to which the data subject is party or in order to take the necessary steps prior to the data subject entering into a contract

Data we hold will, at all times, be processed and stored securely and within the requirements of the General Data Protection Regulations (GDPR) and in accordance with our data security policy.

Governance

Privacy by design is an implicit requirement of data protection and we have a general obligation to implement technical and organisational measures to show that we have considered and integrated data protection into our processing activities.

Our firm understands the importance of having robust governance, systems and controls in place to protect the rights of data subjects and to ensure our on-going compliance with the requirements of the GDPR.

Mr Ian Thornber, Director, has primary responsibility for GDPR ensuring that compliance with the regulations is central to the culture within our business and that all staff are discharging their duties appropriately with regard to personal data. Also, that our Privacy Notice remains accurate and up to date and that we maintain an archive of all Privacy Notices issued.

In addition to regular, proportionate checks and audits of our internal procedures, it is our practice to undertake proportionate enquiries of our third party data processors to ensure they remain compliant with GDPR on an on-going basis.

Mr Ian Thornber discusses annual reports with his fellow Director, Mr Jason Moore:

- GDPR audit results and action points
- Breaches and notifications to ICO/data subjects
- Conflicts of interest
- Staff training and awareness
- Issues arising from our data processors
- Complaints relating to data protection
- Subject access, rectification, erasure and portability requests
- Physical security
- Systems and controls
- Disposal of data
- Compliance and monitoring

Legal Basis

We will ensure that at all times, we are legally able to process, store and share personal identifiable information. Where necessary, for example for marketing purposes or when special category data is involved, we will obtain explicit consent from the data subject.

Personal Identifiable Information is:

- Any information relating to a living person that can be used to directly or indirectly identify that person
- Full name, email address, date of birth, IP address / website cookies
- Purchases, downloads, subscriptions and services used
- Questions and responses, promotions used, survey responses
- Financial history, banking/credit, payment transactions and donations
- Healthcare and education services used
- CCTV recordings, gender identity, location data, credit card data
- Judgements/sanctions, government services
- Capable of identifying an individual either on its own or when combined with other information
- Internal account numbers, PINs and passwords, IMEIs, National Insurance number
- Driving licence number, passport number

Special Category / High Risk Data is:

- Race/ethnic origin, political opinions, religious beliefs and union membership
- Biometric, genetic, health/medical data
- Sexual orientation, sex life
- Criminal offenses, criminal convictions

Consent

Consent must be freely given, unambiguous and on an opt-in, not opt-out basis. Consent must not be a condition of provision of service.

We will ensure that consent for the use of personal data is obtained specifically for each of purpose and separately from consent to any other terms or conditions.

All data subjects will be provided with a copy of, or access to, our Privacy Notice. We will retain an archive of version controlled Privacy Notices.

In order to demonstrate our compliance with the requirements for consent, when consent is given by a data subject, our systems will record the following:

- Name of data subject providing consent
- Date consent obtained
- Method of consent (verbal, E-Mail etc)
- Staff member consent given to
- Version of privacy notice applicable at time of consent

Sharing Data

We acknowledge that it will be necessary to share personal identifiable information, including special category data, with third parties (data processors) in order to facilitate and assist with the on-going performance of a contract with our data subjects. For example, insurers, data storage facilities, HR support providers, payroll services etc.

We will take proportionate steps to ensure that all third parties receiving data from us are compliant with GDPR requirements. We recognise that a failure of one of our data processors to comply with the GDPR directly affects our ability to comply.

Where data is transferred/stored outside the United Kingdom and/or the European Economic Area (EEA), we will take appropriate action to ensure that all countries involved meet the requirements of the GDPR, for example by registering with Privacy Shield (https://www.privacyshield.gov/list). Non-EEA territories considered to have 'adequate protection' under GDPR are Andorra, Argentina, Canada, Faroe Islands, Guernsey, IoM, Israel, Jersey, New Zealand, Switzerland, Uruguay?

Retention of Data

We recognise that the GDPR require us to hold data for no longer than is absolutely necessary. Data will therefore be stored in line with our data retention policy.

Any request from a data subject to have their data erased must be processed taking into account our legal requirements on data retention, as specified by the Financial Conduct Authority, the Companies Act or other legislation, whichever requirement is the longer.

We will take necessary, proportionate steps to ensure that all data we hold is at all times kept secure, both manual and electronically held data, while 'at rest' on our systems, in transit to and stored by any third party. Such measures may include but not be limited to:

- Keeping manual files in locked cabinets when not in use
- Operating a clear desk policy
- Ensuring our firewall and cyber protection remains up to date
- Limiting access to data to only those who need it
- Encryption of data 'at rest' and while in transit, for example by E-Mail, data stick, lap-tops etc.

Deletion of Data

In line with our data retention policy, we will ensure that once the compulsory retention period has passed, data will be destroyed / deleted securely.

In order to achieve this, we have instigated a process to identify data due for deletion and its destruction/removal from our system. This will include secure shredding of manual documentation and deletion of data from our computer systems.

Rights of the Data Subject

We recognise the rights of data subjects provided by the GDPR and these will at all times be respected.

Where a data subject wishes to exercise their right of access or rectification, this will be acted upon promptly but in all cases, no later than 30 days from the date of request. No charge will be make for providing the data subject with the information or the correction of any incorrect or inaccurate information we hold.

Breaches

The GDPR places on firms the obligation to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we must notify the data subject concerned directly.

A 'high risk' means the threshold for notifying individuals is higher than for notifying the ICO.

If a breach has been identified, it must be reported immediately to Mr Ian Thornber, Director, who is responsible for investigating and reporting breaches. We have a system in place for reporting breaches in order to identify:

- How the breach occurred
- When it happened and how long it was happening for
- What categories of data were involved
- Number of records/data subjects affected
- How we have mitigated the breach

Once the above information has been obtained, but in all cases not longer than 72 hours from when we became aware of the breach, notification of the breach will be made by Mr Ian Thornber, Director, to the ICO, and if appropriate, to the data subject.

Full details of the breach, investigation and notifications will be shared with all Directors.

This policy and processes arising from it are reviewed annually by Mr Ian Thornber, Director & Mr Jason Moore, Director, G. Moore & Co. Ltd, 2 Albion Street, Cross Roads, Keighley, West Yorkshire, BD22 9EB.