320 City Road, London, EC1V 2NZ, UK,
www.quantemol.com, Registered number 0 5 0 4 8 1 8 4

QUANTEMOL PRIVACY POLICY

Within Quantemol's business operation, we collect information about our customers for four main reasons:

1. To offer our software and services to relevant businesses.
2. To provide continuous support and the best levels of service to our current customers.
3. To conduct market research helping to identify R&D strategy for Quantemol products development and new markets identification.
4. Only with the consent of each customer (by signing up for a newsletter) to send email marketing communications updating on recent Quantemol product developments and relevant events.

Version 1.0
Issue date 20 April 2023
Prepared by A. Nelson

Principles

Quantemol does its utmost to protect your privacy through the appropriate use of security technology. This means:

- We aim to ensure that we have appropriate physical and technological security measures in place to protect your information.
- We aim to ensure that when we use other service providers for any processes, these service providers also have appropriate security measures in place to protect your information.
- Quantemol respects your privacy. You should only receive marketing emails from Quantemol which you have agreed to. It will be made clear to you where you have these choices.
- Quantemol will only collect and use your information where we have legitimate business reasons, and we are legally entitled to do so.
- Quantemol will be transparent about the information we will collect on you and how we will use your information.
- Quantemol will only use your information for the purpose(s) for which they were originally collected and we will ensure any old information is securely disposed of.

How Quantemol may collect your Personal Information

We collect information in the following ways:
When you give it to us DIRECTLY: You may give us your information when you:

• Sign up as a QuantemolDB member via an online form
• Sign up for one of our events
• Use one of our services
• Communicate with us generally via email or social media
• Provide us with specific consent to contact you for given purposes at a conference

When you give it to us INDIRECTLY: Your information may be shared with us by a third party. For example, you may be recommended by a colleague, or by being referred to us for your expert knowledge by other experts in the field.

When you share your information or it is available publicly we may combine the information you provide to us with information available from external sources in order to gain a better understanding of your field of expertise to perform a Legitimate Interests Assessment with the purpose of contacting you with our business offers.

Personal Information you share with us

“Personal Identifiable Information" is the information that identifies you as an individual, such as name, postal address, telephone number, and email address. Quantemol collects Personal Information only when you submit it to us.

Your information will be located in the Quantemol CRM system. The data is encrypted using industry-standard AES-256 and SOC 2 compliant, and it has world-class data storage. There are advanced user permissions, two-factor authentication, SAML SSO logins and more. All customer data is encrypted in transit over public networks using Transport Layer Security (TLS) 1.2/1.3 with Perfect Forward Secrecy (PFS) to protect it from unauthorized disclosure or modification.

Quantemol mitigates the internal risk of unauthorised access to your personal data by restricting access to CRM only to employees who are directly related to customer relations.

Your personal data will be stored for 5 years after the last project we conducted with you or the last contact where you indicated potential interest in working with Quantemol in future and removed afterwards. We will not share your information with any third parties.

Customer discussion records

After you have shared with us your project details or purposes for the software use in order to enable us to provide you with the best service a record will be created and your information will be stored in an encrypted format on the Quantemol cloud server, CRM and if any email communications were provided stored encrypted in the email server.
Only relevant employees have access to it in order to utilise it to enhance our business suffering or support for you. The records will be deleted after 10 years after the last project we conducted with you or the last contact where you indicated potential interest in working with Quantemol in future and removed afterwards.

How the information will be used

The information you provide will be kept confidential and not reused for any other purposes than the current project.

The discussion records will be kept in order to analyse your answers and offer the best services relevant to your needs. The insight will help us to evaluate how our technology can aid your research and where we can spot potential R&D developments to improve our offering

Your personal data will be kept in order to organise further discussions and potential future contact about our product developments, should you opt-in to be kept updated.

You have the following rights with regard to your personal information:

- the right to be informed about the collection and use of your personal data
- the right to access personal data and supplementary information
- the right to have inaccurate personal data rectified, or completed if it is incomplete
- the right to erasure (to be forgotten) in certain circumstances
- the right to restrict processing in certain circumstances
- the right to object to processing in certain circumstances
- the right to withdraw consent at any time
- the right to complain to the Information Commissioner

Updating your personal information

The participants have the right to ask to access, rectify, delete, export and restrict their data from being processed. Quantemol will update your personal information at any time, including email, phone, affiliation and subscriptions within 72 hours of you requesting the changes via support@quantemol.com.

Data Deletion Policy

All the stored personal data will be deleted 5 years after the latest project completion or contact from your side.

DPO can delete data from the CRM system. This data is deleted from the system immediately and cannot be recovered by any Quantemol employees after this point. Data which has been deleted or otherwise destroyed can not be recovered at any time. Data remaining in the system's backup files will be deleted periodically (every 2 years).

Information may be deleted from our CRM upon request to support@quantemol.com. We undertake to perform the complete deletion from CRM and all the backup files within one month (30 calendar days) and will send you a confirmation once the information has been deleted. Wherever possible, we will aim to complete the request in advance of the deadline.

Legal information

Please note that Quantemol reserves the right to access and disclose personal data to comply with applicable laws and lawful government requests.

Changes to the privacy statement

Should Quantemol select to change the Quantemol Privacy Statement, we may choose to email all our customers with the new details. Where required by law, we will obtain your consent to make these changes.

Data Protection Act Registration

Quantemol is registered with the Information Commissioner's Office under registration reference ZA205556.

Data security

We will use appropriate technical and organisational measures to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Who is responsible for data protection and IT security?

Maintaining appropriate standards of data protection and data security is a collective task shared between us and you.

This policy and the rules contained in it apply to all staff of Quantemol, irrespective of seniority, tenure and working hours, including all employees, directors and officers, consultants and contractors, casual or agency staff, trainees, homeworkers and fixed-term staff and any volunteers (Staff).

Questions about this policy, or requests for further information, should be directed to the Data Protection Officer.

All Staff have a personal responsibility to ensure compliance with this policy, to handle all personal data consistently with the principles set out here and to ensure that measures are taken to protect the data security. Managers have special responsibility for leading by example and monitoring and enforcing compliance.

The Data Protection Officer must be notified if this policy has not been followed, or if it is suspected this policy has not been followed, as soon as reasonably practicable.

Any breach of this policy will be taken seriously and may result in disciplinary action up to and including dismissal. Significant or deliberate breaches, such as accessing any data types without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Maintaining data security means making sure that:

- Data is only available on a need-to-know basis
- only people who are authorised to use the information can access it;
- where possible, personal data is encrypted;
- information is accurate and suitable for the purpose for which it is processed; and
- authorised persons can access information if they need it for authorised purposes.

By law, we must use procedures and technology to secure personal information throughout the period that we hold or control it, from obtaining to destroying the information.

Personal information must not be transferred to any person to process (eg while performing services for us on or our behalf), unless that person has either agreed to comply with this data protection or we are satisfied that other adequate measures exist.

Quantemol security procedures include:

- Any desk or cupboard containing confidential information must be kept locked.
- Computers should be locked with a strong password that is changed regularly or shut down when they are left unattended and discretion should be used when viewing personal information on a monitor to ensure that it is not visible to others.
- Any other passwords to platforms with Personal data must be changed from the default, updated regularly and be different across all platforms
- Data stored on cloud severe must be encrypted or password protected and locked away securely when they are not being used.
- Passwords must be non-guessable (avoiding any continuous number or letter strings, obvious words like “password” and strings that lie next to each other on a keyboard like “querty”)
- Whenever possible, passwords will be generated by and stored in a password manager approved by Quantemol e.g. Chrome, Dashline or 1Password.
- Only use Google Drive and Dropbox to store electronic data.
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
- All servers containing sensitive personal data must be approved and protected by security software.
- Servers containing personal data must be kept in a secure location, away from general office space.
- Data should be regularly backed up in line with Quantemol's backup procedure.
- Additional software not on **the software register** must be signed off by senior management before the installation

Telephone Precautions. Particular care must be taken by Staff who deal with telephone enquiries to avoid inappropriate disclosures. In particular:

- the identity of any telephone caller must be verified before any personal information is disclosed;
- if the caller's identity cannot be verified satisfactorily then they should be asked to put their query in writing;
- do not allow callers to bully you into disclosing information. In case of any problems or uncertainty, contact the Data Protection Officer.

Methods of disposal: Copies of personal information, whether on paper or on any physical storage device, must be physically destroyed when they are no longer needed. Paper documents should be shredded and CDs, memory sticks, laptops or similar must be rendered permanently unreadable.

Data protection impact assessments

Where processing would result in a high risk to Staff rights and freedoms, Quantemol will carry out a data protection impact assessment (DPIA) to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data breaches

If we discover that there has been a breach of Staff personal data that poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner within 72 hours of discovery.

We will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to your rights and freedoms, we will tell affected individuals that there has been a breach and provide them with more information about its likely consequences and the mitigation measures it has taken.

Individual responsibilities

Staff are responsible for helping Quantemol keep their personal data up to date.

Staff should let Quantemol know if personal data provided to Quantemol changes, e.g. if you move house or change your bank details.

You may have access to the personal data of other Staff members and of our customers in the course of your employment. Where this is the case, Quantemol relies on Staff members to help meet its data protection obligations to Staff and to customers.

Individuals who have access to data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose personal data except to individuals (whether inside or outside of Quantemol) who have appropriate authorisation;
- to keep personal data secure (eg by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);

- not to remove personal data, or devices containing or that can be used to access personal data, from Quantemol's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Appendix

DPO Role description

Quantemol has appointed CEO, Anna Nelson as a Data Processing Officer to ensure compliance of our data processing with GDPR standards and establish a Data Processing Impact Assessment (DPIA).

DPO duties include:

- Monitoring compliance with the GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits.
- Provide advice and information on Quantemol data protection obligations.
- Monitor a DPIA.
- Assess risks associated with processing operations, and take into account the nature, scope, context and purposes of the processing.
- Act as a contact point for the ICO.