Our Privacy Notice

Who we are: We are Quantios Management Services Limited ("Quantios") registered in England and Wales under number 12003494 with registered office Sentinel House, Harvest Crescent, Fleet, England, GU51 2UZ. Quantios group ("Quantios Group") comprises Quantios any entity that directly or indirectly controls, is controlled by or is under common control with Quantios. In this Privacy Notice "us", "our", "we" refers to Quantios Group.

About Our Privacy Notice: Our Privacy Notice (our "Privacy Notice") describes our collection, use, disclosure, retention and protection of your personal information. Our Privacy Notice applies to any website, application or service which references it and to all applications and services offered by us that do not have a separate privacy notice for which we are responsible for controlling or processing personal data.

Data Controller/ Data Processors: Quantios is the Data Controller within Quantios Group. When handling personal data, Quantios subsidiary companies act as a Data Processor to Quantios.

When we collect personal information: Quantios collects information from or about individuals when:

- they are an actual or potential customer, consultant, supplier, advisor or business partner or associate of us;
- they are an employee, employee equivalent or prospective employee interested in joining us;
- they visit our websites, sign up to our news notifications via any registration form on our website, or they engage with us on social media;
- they contact us by any means with queries, interests or concerns or complete our surveys whether we have sent such surveys to them directly;
- they have a meeting or appointment with us or attend any of our events including in person at a venue or online;
- they visit one of our offices where there identification details and image may be recorded; and
- they elect to provide us with personal information during business encounters, for example by email or business card.

We collect personal information from individuals directly, from public sources or from third parties, such as business associates or recruitment agents.

Personal data we collect and the Purpose:

The category labels we use for personal are as follows:

Category of personal data	Examples
General Data	Phone numbers, business and private, work addresses, location. electronic signatures, correspondence, job title, line manager, employer name, functional division in the employer, biographies, career history, bought in data, username and similar data that might identify a person.
Sensitive Data	Sensitive personal data relating to confidential, private and medial details, details of protected characteristics e.g. hand written signatures, gender, family information, beneficiaries, marital status, salary data.
Identity Verification	Passport/ drivers licence, residential addresses, proof of address nationality, age, date of birth and other details required for Know Your Customer, anti-money laundering, references, background checks and other similar checks.
Financial Data	Bank account and payment details, bank details, data on transactions with us, credit reports, financial reports, national insurance and tax

	codes, timesheets etc that identify or are information pertaining to an Individual.
Visual Data	Photos, videos and meeting recordings and sound recordings.
Preferences	Dietary requirements, opt-in and opt-out consents, and other information individuals provide to us relevant to the services we provide.
Cookie Data	Cookies collected automatically by visiting our websites including domain name, IP address, operating system and browser.
Device Data	Device identification number and type, location information and connection information such as statistics on page views, traffic to and from the sites, referral URL, ad data, IP address, MAC Address, Device Name, location, browsing history and web log information
HR Data	Personal data in addition to above collected by our Human Resources related to individuals working with us.
Anonymised Data	Any of the above where personal identifiable data has been redacted or encrypted to leave date that is not identifiable with an individual.

The category of personal information that we collect depends on the legitimate purposes for which it is collected as follows:

Activity/ person	Category of personal data we collect or use	Purpose	Lawful basis for processing
Customers of our applications and services.	General Data Preferences	To provide software and services under contract. If required by customers, we will use their handwritten signature (Sensitive Data) and may charge for this as an additional service.	Contract Legitimate Interest
Prospective customers.	General Data Preferences Visual Data	To provide product demonstrations to customers, typically working under an NDA.	Consent
Customer Clients	Anonymised Data.	To fulfil specific contract obligation directed by customers.	Contract
Users of our applications and services.	General Data Preferences Cookie Data Device Data	To provide software and services under contract. This include where we provide hosted services.	Contract Legitimate Interest
Technical bulletins to customers on licenced software and software feedback surveys.	General Data Preference Data	To provide software and services under contract. We will respect opt-outs.	Legitimate Interest Contract
Marketing activities such as market bulletins, online surveys, new letters, and event invitations.	General Data Preference Data Cookie Data Device Data	To provide information on our software and services to develop our business.	Consent

Events such as product launches and technical updates.	General Data, Preferences, Visual Data	To provide information on our software and services to develop our business.	Consent
Dialogue arising from contacting us offline by telephone, email, post etc	General Data Preferences	To provide individuals with support and assistance in order to develop our business.	Consent
Analysis of website usage, marketing and business performance data.	Anonymised Data	To help us to monitor and improve our business and the services and software we provide.	Legitimate Interest
Browsing our websites.	Cookie Data Device Data	To help us understand the use of our website and interest in our products. To enable monitoring and improvement of our website.	Consent
Interacting with us using social media.	General Data Cookie Data Device Data	To provide individuals with support and assistance in order to develop our business	Consent
Our suppliers	General Data Financial Data Cookie Data Device Data	To purchase products and services from suppliers and to monitor the performance of suppliers	Contract Legitimate Interest
Business administration	General Data Sensitive Data Identity Verification Visual Data Preferences Cookie Data Device Data HR Data Anonymised Data	To fulfil our legal and contractual obligation for administering the business properly, efficiently and effectively	Consent Contract Legal Obligation Legitimate Interest
Our employees and people applying to work for us	General Data Sensitive Data Identity Verification Visual Data Preferences Cookie Data Device Data HR Data Anonymised Data	To fulfil our legal and contractual obligations for employees and our business.	Consent Contract Legal Obligation Legitimate Interest

The lawful bases for processing used in the table above are set out in Article 6 of the UK GDPR and are:

- **Consent**: the individual has given clear consent to process their personal data for a specific purpose;
- **Contract**: the processing is necessary for a contract that we have with the individual, or because they have asked us to take specific steps before entering into a contract;

- **Legal Obligation**: the processing is necessary for us to comply with the law (not including contractual obligations) such as compliance with legal and regulatory obligations; requests for disclosures from a court, tribunal, authority, regulator or supervisory or governmental body; and
- **Legitimate Interests**: the processing is necessary for Quantios Group's 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.

If you would like further information on how we have balanced our and others' legitimate interests against your privacy interests, please contact privacy@quantios.com.

We may use personal information for the purposes of the following legitimate interests:

Activity/ person	Legitimate Interest
Business operations:	• provide, maintain, protect and improve our services and applications purchased/ licenced from us and manage and administer use of them; • monitor, measure, improve and protect our content, website, applications and services and provide an enhanced, personal, user experience for you; • manage the relationship with and performance of our suppliers; • detect, prevent, investigate or remediate, crime, illegal or prohibited activities or to otherwise protect our legal rights (including voluntary liaison with regulators and law enforcement agencies for these purposes); • perform activities relating to customer management, financial management, reporting and administration (such as promotion of our business to potential clients, performing accounting, other internal functions and audit); • compliance with Know Your Customer and anti-money laundering requirements and references, background and other similar checks on or conducted by or on us; • obtaining professional services from our lawyers, accountants, consultants and auditors.
Customer relationship management and business development	• facilitating business opportunities, including communicating with individuals about potential business, partnership or career opportunities; administering relationships, meetings and travels for employees, customers and business partners; • manage relationships with customers; • contact customers to see if they would like to take part in our customer research (for example, feedback on their use of our applications and services); • providing publications that are appropriately focused and may improve their use of our software and services, including communicating with individuals about service updates, responding to enquiries and resolving complaints; • monitor, carry out statistical analysis and benchmarking on our customer base; • monitoring use the use of our website and social media channels to improve our marketing materials and activities.
Employees and Candidates	• perform all our business operations, such as for payroll and for managing staff; • recruitment activities for us, including assessing candidate application for employment with us; evaluating potential candidates for

	recruitment processes; background checks to ensure the suitability such as criminal record checks and obtaining references; • maintain records on past employees that may be require e.g. to resolve pension queries and to provide references; • retain records in accordance with our information retention policy for candidates who may be suitable for future roles with us.

We may enhance personal information we collect from you with information we obtain from third parties that are entitled to share that information; for example, information from sanction lists, credit agencies, search information providers or public sources (e.g. for customer due diligence purposes), but in each case as permitted by applicable laws.

We may monitor and record our communications with you.

Our use of Cookies

For further information about our use of cookies, please see our Cookies Notice a link for which is found as the end of pages of our website.

You may be able to configure your browser or our website, application or service to restrict cookies or block all cookies, but you may find this affects your ability to use certain parts of our website, applications or services. If you would prefer to block cookies please refer to the instructions or help service on your internet browser.

Who we share personal information with

(a) Quantios Group: Quantios Group entities, acting for Quantios as Data Controller, share personal information within other Quantios Group entities.

(b) Third-party providers: We may share personal information with trusted third parties, including independent contractors or subcontractors (such as individuals who are engaged to assist Quantios Group on specific projects), agents (such as recruitment agents and corporate secretarial services agents) and service providers (such as legal, consultancy, background screening providers and providers we use for other outsourced business administration suppport) who need to receive the personal information in order to provide services for and on behalf of us for the purposes specified in this Privacy Notice.

We engage trusted third-party IT service and software providers such as Microsoft to host, store and process data, e.g. information relating to employees is stored on a cloud-based HR software system; information about employment candidates is recorded on a cloud based recruitment system; supplier and customer information is processed on systems for accounting, management reporting, project management and on other systems.

We may share personal information in accordance with the express consent of an individual, what the individual has given such consent, or a Data Processing Agreement.

Information will only be transferred or provided to third-party providers where reasonably necessary to enable us to fulfil the purposes set out in this Privacy Notice. We will ensure that each such provider has agreed to protect and maintain the confidentiality and security of information we share with them.

(c) Our ownership: We may share certain personal information with an actual or potential buyer, seller, co-investor or joint venture partner and our and their advisers in connection with any actual or potential acquisition, sale, co-investment, joint venture or similar transactions in connection with Quantios Group. Sharing such information if made would be limited to what is necessary and safeguards would be implemented such as confidentiality agreements and agreements to restrict the use of the information to purpose of the transaction.

Authorities as required or permitted by law

We may disclose personal information: (a) as required or permitted by, or to comply with, applicable law, regulation, court or tribunal processes or other statutory requirements; (b) to respond to requests from or disclosures required by any court, tribunal, authority, regulator or supervisory or governmental body or (c) to comply with Know Your Customer and anti-money laundering requirements and references, background and other similar checks on or conducted by Quantios Group.

Providing us with personal information about other individuals

If you provide us with personal information about someone else, you are responsible for ensuring that you comply with any obligation and consent obligations under applicable data protection laws in relation to such disclosure. In so far as required by applicable data protection laws, you must ensure that you have provided the required notices and have obtained the individual's explicit consent to provide us with the information and that you explain to them how we collect, use, disclose and retain their personal information or direct them to read our Privacy Notice.

Our standard retention period

The personal data we collect will only be retained for as long as it is needed to fulfil the purposes set out in this privacy statement. This period is maximum 10 years, subject to certain variations described below.

Deletions will be carried out in accordance with Quantios's retention policy. Any information stored in hard copy format (in paper form) is treated as confidential and will be shredded when we no longer have a legitimate interest in retaining it and may not seek your permission to destroy it.

Variations to the retention period

We will retain your information for longer than the standard retention period where permitted or required by law, including to comply with the duration of any statutory or contractual limitation periods. For example, we will retain copies of contracts with customers for as long as permitted by law.

In relation to data collected about visitors to the website, data is retained for 50 weeks.

In relation to personal data collected about potential employment candidates who we do not hire the data may be retained for up to six years in case such candidates are suitable for other employment opportunities which arise at with us.

Data privacy rights of Individuals

Data protection laws in some countries provide data subjects with various rights. In the European Union and United Kingdom, data protection laws provide rights to:

Data Subject Rights	
The right to be informed	Individuals have the right to be informed about the collection and use of their personal data. This is commonly referred to as a subject access request or 'SAR'.
The right of access	Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
The right to rectification	Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete. Individuals may ask us to **correct** the information that we hold about them.
The right to erasure	Individuals have the right to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. Individuals may

	require us to remove them from our marketing lists or change your marketing preferences by contacting privacy@quantios.com;
The right to restrict processing	Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, we may store the personal data, but not use it.
The right to data portability	Individuals have the right to data portability so that they can obtain and reuse their personal data for their own purposes across different services. Individuals may request a copy of the information we hold about them by email to privacy@quantios.com;
The right to object	Individuals have the right to object to the processing of their personal data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing.
Rights in relation to automated decision making and profiling	Individuals have rights for: (i) automated individual decision-making (making a decision solely by automated means without any human involvement); and (ii) profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process. We use profiling for market analysis and for prioritising and filtering prospective customers for our sales activities, but decisions are made by human intervention.

Your rights regarding your personal data are not absolute and may not apply in all circumstances. In some cases, exemptions may apply. When you make a request to exercise your rights, we may need to verify your identity to ensure the security of your data. We will ask for information necessary to confirm your identity and to fully understand the nature of your request. If, for any reason, we are unable to fulfill your request, we will provide a detailed explanation as to why.

To exercise any of your rights, including making a Subject Access Request (SAR), or if you have any questions about how we handle your personal information, please contact us via email at privacy@quantios.com. Alternatively, you can send a letter to our postal address listed in the 'Further Information and Contacting Us' section below. We commit to responding to your SAR and any other rights requests promptly and no later than one month from the date we receive your request. If your request is particularly complex or if you have made multiple requests, we may extend this period by up to two additional months, and we will inform you of this extension and the reasons for the delay within the first month.

Transferring information internationally

We are a global business and have offices in various countries (see here: https://quantios.com/contact-us/), use global systems and interact with other parties globally. For example, we engage third-party IT service and software providers which host, store and process data in and outside of the European Economic Area (the "**EEA**") and the United Kingdom (the "**UK**"). This means that your information may be transferred to a country outside the EEA – such as the US and other non-EEA countries or to a country outside the UK. These countries may not offer the same level of data protection as in an Individuals home country, and may not be deemed as providing an adequate level of data protection under applicable data protection laws ("Non-Adequate Countries"). Where personal information is transferred from within the EEA or from within the UK to a Non-Adequate Country, care is taken to ensure that the transfer is subject to appropriate safeguards per applicable data protection laws. Such

safeguards include standard contractual clauses and adequacy decisions. Our first safeguard is to avoid transferring data unless necessary.

Each company within our group is bound by an agreement that includes standard contractual clauses. This agreement governs the transfer of personal data between the group companies to ensure compliance and protection of your information.

Security

We are committed to ensuring that personal information is secure. As an ISO 27001 certified organization, we adhere to stringent standards for data security. Our information security management system includes physical, electronic, and managerial measures designed to prevent unauthorized access and disclosure of personal information. These safeguards include encryption, secure data storage, and controlled access for authorized personnel only. We also conduct security training for our employees and undertake periodic risk assessments and audits to enhance our security protocols. While we implement robust precautions to protect data, it is important to acknowledge that no method of transmission over the internet is completely secure. We strive to protect your information, but absolute security cannot be guaranteed.

Automated Decision-Making:

We use automated decision-making in some areas of our business to improve operational efficiency. These processes can involve assessing eligibility for services or analysing customer interactions and data. Although decisions may be made automatically, we ensure accuracy and fairness through established safeguards. Given the growth of artificial intelligence tools we are likely to make increasing the use of these tools. For any concerns or additional information, please feel free to contact us. If an automated decision affects you, you have the right to request human intervention, express your point of view, and challenge the decision.

Review and Changes to Our Privacy Notice

We regularly review and may update our Privacy Notice to ensure it accurately reflects our current practices and complies with legal requirements. This review occurs annually and whenever significant changes to our business processes or data handling practices occur, or when new legal regulations are enacted. We are committed to maintaining transparency and protecting your privacy, and we encourage you to review our Privacy Notice periodically to stay informed of any updates.

Other sites and social media

If you follow a link from our website, application or service to another site or service, Our Privacy Notice will no longer apply. We are not responsible for the information handling practices of third-party sites or services.

Further information and contacting us

If you have any queries about how we treat your information, the contents of this Privacy Notice, your rights, how to update your records or how to obtain a copy of the information that we hold about you, please email privacy@quantios.com or write to

Company Secretary and Compliance Officer,
Quantios,
Sentinel House, Harvest Crescent,
Ancells Business Park,
Fleet,
United Kingom, GU51 2UZ.

Our Data Protection Officer may be contacted at michael.daykin@quantios.com (Company Secretary and Compliance Officer).

May 2024