The General Data Protection Regulation ("GDPR") is the new legal framework that will come into effect on the 25th of May 2018 in the European Union ("EU") and will be directly applicable in all EU Member States from that date.

The GDPR's focus is the protection of personal data, i.e. data about individuals, and builds on existing data protection laws, setting out the responsibilities of businesses in relation to the personal data they collect, hold, transmit and otherwise use. The GDPR is extra-territorial in nature and applies not just to organizations within the EU who process the data of individuals but also organizations outside the EU who offer goods or services to individuals in the EU, or who monitor the behaviour of individuals in the EU. Because the EU is a trading partner of most countries, the GDPR's wider scope means it has implications for many businesses worldwide and will effectively require them to be compliant if they wish to operate in EU member states either directly or as a third-party for others.

Clarity Business Software Limited – GDPR Statement of Compliance

The General Data Protection Regulation ('GDPR') is effective from 25th May 2018.
In preparation for GDPR, Clarity Business Software Limited ('Clarity') acknowledges its responsibility to develop and maintain business-wide awareness of the rights of individuals to be empowered and protected in terms of data privacy.

We have consulted broadly and implemented processes, procedures and training to ensure that a legal basis for the processing of personal data underpins all business practices at Clarity. We recognise that there are a small number of circumstances in which personal data may be processed and that the GDPR clarifies the responsibilities of companies as far as the processing (collection, storage, maintenance and use) of personal data is concerned.

Clarity is actively working on its GDPR strategy and considers this to be an ongoing endeavour that will continue to be operational beyond the enforcement date of 25th May 2018. We will continually strive to ensure that personal data privacy is embedded as routine practice on a perpetual basis.

Clarity has undertaken to ensure that all staff receive training in the concepts and requirements of data protection law. Staff will be expected to embrace the ethos of data protection law and to adopt practices in the workplace that reflect the company's commitment to ensuring that the rights of individuals are respected and protected always.

Clarity's' internal policy for data protection requires any products, services or systems adopted by the company (relating in any way to the processing of personal data) to undergo an assessment to establish that they do not contravene the company's policies to maintain compliance with the GDPR.

FAQ

Where and how will the data about me be recorded?

- We will collect and store information about you when you; enquire about our products and services via an online form or by telephone; when you email us or when you meet with us.
- Your data is likely to be recorded in our Customer Relationship Management (CRM) database system. There may also be emails that you have sent to us (and that we have sent to you) recorded in our CRM system and within our email server database. It is probable that we will hold a record which relates to you within our accounting software database as well.
- Our CRM, Email and Accounting databases are all maintained within a secure location in the European Union.
- We may also record your email address, name and company name in our mass email broadcasting system (which is a secure cloud-based database).

What data do Clarity hold about me?

Our CRM system is configured to provide for the recording of the following personal information:

- Full name
- Name Prefix
- Title
- Type of Role
- Any preference which you have expressed relating to the receipt of marketing materials from us via email or direct mail
- Phone number(s)
- Email address(es)
- Postal address (usually a business address, unless you work from home)

In addition, we may have attached to your record in our CRM system:

- Documents that you have sent us
- Emails that you may have sent to us or we have sent to you
- Notes that we have made as outcomes from interactions with you (telephone conversations and meetings)
- Details of any future planned activities that we have with you
- Records held within our accounting system will include a history of transactions (including sales orders, invoices and financial status information that relates specifically to your trading history with us). These may be regarded as 'personal' if you are a sole trader or a corporate entity of some kind.

How does Clarity ensure data security?

- All our database systems are password protected and access is only afforded to those with a legitimate reason for so doing.
- All users are required to have a domain user name and password to authenticate against the security model for access to our databases. Password policies determine that these must be changed with a high degree of frequency and they must also have a pre-determined level of complexity.
- Remote workers are only able to access data services within our corporate network via secure Virtual Private Network (VPN).

What do you do with my information?

We use your information for the following purposes:

- To communicate with you in relation to the products and services that your employer has contracted with us to provide.
- To monitor our levels of customer service and manage the way in which we support you (if your employer is our customer).
- To understand our customers' needs and requirements.
- To advise you of other products and services that we offer which we feel may be of benefit to you and/or your employer.
- To alert you to events and news that we feel might be relevant and/or useful to you.

With whom do you share my information?

We will never share your information with a third party without your express permission unless we are required to do so by law.

Do you process sensitive personal data?

We do not directly process data which the Data Protection Act 1998 defines as 'sensitive personal data'. As a business to business (B2B) company, most data recorded within our systems is of a corporate nature.

How will you use my information to contact me?

We may contact you by telephone (via a business phone number where it has been provided, and sometimes via a mobile phone), by post (to your business address), by email (via a business email address if you have provided us with one) or by Social Media platform (such as LinkedIn, Facebook or Twitter).

Will you send me marketing information?

We will only send you marketing information about other products and services that we (ourselves) offer. Most of our marketing communications are broadcast via an email marketing platform. This platform includes an 'unsubscribe' link. You may use this link to inform us that you no longer wish to receive email marketing messages from us or you may alert us to this via phone on 01761 231 399, or by email: info@claritybusinesssoftware.co.uk or in writing (to our office address: The Apple Store, Coombe Lodge, Blagdon BS40 7RG).

Can I see the information that you hold about me?
If you would like a copy of the personal information that we hold about you, simply call us on 01761 231 399 or write to us at Clarity Business Software Limited, The Apple Store, Coombe Lodge, Blagdon, BS40 7RG. We will acknowledge the request as soon as we receive it and will provide a full response within 40 calendar days of our acknowledgement.

Clarity as a Data Controller

System Access Control:

- We ensure that all systems processing personal data (this includes remote access) are password protected after boot sequences, when left for even a short period of time, preventing unauthorized persons from accessing any personal data.
- We provide dedicated user ID's for authentication against systems user management for every individual, assigning individual passwords, ensuring that access control is supported by an authentication system.
- We make sure that controls to grant access to authorized personnel and to assign only the minimum permissions necessary for those personal to access personal data in the performance of their function.
- We have implemented a password policy that prohibits the sharing of passwords, outlines processes after a disclosure of a password and requires the regular change of passwords.
- We have implemented a proper procedure to deactivate user account when a user leaves the company or function.
- We have implemented a proper process to adjust administrator permissions when an administrator leaves company or function.
- We have implemented a process to log all access to systems and review those logs for security incidents.

Data Access Control:

- Persons entitled to use a data processing system shall gain access only to the data to which they have a right of access, and a personal data must not be read, copied, modified or removed without authorization during processing. We have implemented the following controls:
- Restricted access to files and programs based on a 'need to know basis'
- We have controls in place to prevent use/installation of unauthorized hardware and/or software.
- We have established rules for the safe and permanent destruction of data that are no longer required.
- We have controls to grant access only to authorized personnel and to assign only the minimum permissions necessary for those personal to access personal data in the performance of their function.

Clarity as a Processor

There may be occasions when we will may need to access or take a copy of your data which will include personal data that you control for the following reasons:

- Data conversion during upgrade of software
- Data testing for bespoke development
- Support services

We will only obtain this data with consent and it will only be retained for the purpose it was obtained. Once the purpose for which the data was obtained is completed the data will either be deleted or returned to the client.

Obligations of the Client:

The client shall:

- Comply with the General Data Protection Regulation in relation to its performance of the Processing, in such a way as to not expose Clarity to any violation of the General Data Protection Regulation:
- Process programme data as a processor on behalf of and only in accordance with the instructions of Clarity and only for the purposes of performing the Agreement and determined by Clarity.
- Promptly inform Clarity if the client cannot provide such compliance for whatever reason of its inability to comply, in which case Clarity reserves the right to immediately and automatically suspend processing.
- Not modify, amend or alter the contents of the programme Data unless the client has the prior consent of Clarity.
- Maintain a record of all categories of Processing activities carried out on behalf of Clarity in the performance of this agreement.
- Notify Clarity in writing (by sending an email to the following address): info@claritybusinesssoftware.co.uk regarding any request received directly from a Data Subject and not later than 48 hours after receiving such a request and shall provide reasonable assistance to the Data Subject in order to respond to such Data Subject request.

Security and confidentiality measures:

- During the term of this Agreement, the client shall implement and maintain an up to date training and awareness program for its employees and sub processors regarding Personal Data Security. The client shall ensure that the authorised persons are properly trained in the Processing of Personal Data and only have access to the Programme Data on a need-to-know basis subject to obligation of confidentiality. The Processor shall also take steps to ensure that the authorised persons do not process the Programme Data except on instructions from Clarity unless the client is required to do so by Union or Member State Law.
- The client shall require that any authorised persons entrusted with Processing Programme Data hereunder have undertaken to comply with the principle of confidentially and have been duly instructed about General Data Protection Regulation.

Sub-processors:
The client shall not disclose or permit the disclosure of Programme data to any Third Party and/or shall not subcontract whole or part of the Processing to any Third Party unless the Client has the prior written consent of Clarity as required by Member State Law or the Law of the European Union.

Personal Data Breach:

- In the event of a Personal Data Breach arising during the Processing of the Programme Data by the Client, the Client shall, at its own cost;
- Notify Clarity in writing by sending an email to: info@claritybusinesssoftware.co.uk about the personal Data Breach within 72 hours of becoming aware of it and provide information about the nature of the breach , the name and contact information of the data protection officer or other contact point where more information can be obtained, the likely consequences of the Breach and the measures taken to address the breach.
- The Client should take such actions as may be necessary or reasonably expected by Clarity to minimise the Breach.
- Maintain any record of all information relating to the breach, including the results of its own investigations and authorities' investigations.
- Cooperate with Clarity and take all measures as necessary to prevent future Breach from occurring again.

Evidence and Audit rights:

- The Client shall provide, upon request of Clarity, all information necessary to demonstrate compliance with obligations laid down in this agreement.
- Upon reasonable notice to the Client, Clarity may audit the Client's compliance with the Client's obligations under this Agreement or with any applicable data protection law or regulation. The Client will allow for, contribute to and help Clarity with the audit. The Client will give Clarity access to its facilities, offices and any information necessary to Clarity to evaluate the Clients compliance.