GDPR information sheet for clients

We aim to be clear and transparent about why and how we collect, store and process personal data in order to carry out Churchill Hui's business activities.

In line with GDPR requirements, we strive to:

- Process data in a manner that is compatible with what it was collected for and in accordance with the rights of the data subject
- Only collect the minimum amount of data necessary
- Take steps to ensure data is accurate and up to date
- Only store data for as long as it is necessary
- Ensure we have appropriate technical and organisational measures to keep data secure and confidential
- Carry out due diligence concerning all third parties who process personal information on our behalf

The data controller is Churchill Hui Ltd, registered in England and Wales, Co. No. 07829078. Registered Address: Grosvenor House, 4–7 Station Road, Sunbury, TW16 6SB.

What personal data do we **store?**

We primarily store business contact information for our clients, prospective clients and their staff, such as an office address, job title, business email and contact telephone numbers. We do not request or hold non-essential or sensitive information.

There are some situations where we will store personal contact information which has been provided by an end user, for example if their home address or email address is also their business address.

We act as the controller for the above information.

How do we store **personal information?**

Personal and technical information is stored within the environment owned and managed by Mimecast and Ramsac hosted within our offices and at a secure datacentre facility. It is also held within selected cloud-based services, primarily Mailchimp for sending email communications such as newsletters, event invitations, general business updates and marketing of relevant Churchill Hui services.

Our main application is Rapport/Gekko, which acts as our customer information database. Rapport is a cloud-based solution hosted and managed by Cubic Interactive Ltd, who are responsible for the security of the platform. This is explained further in the next section.

We have received confirmation from all third parties who process personal information on our behalf that either they are already GDPR-compliant, or they will be compliant by the deadline.

We will of course ensure that all third parties are fully compliant by 25th May 2018.

Our systems are protected by multiple layers of security. The server is protected by a SonicWALL firewall, email is scanned by Mimecast and Office 365, and all machines, devices and servers are protected using McAfee anti-virus / anti-malware software.

Next generation firewalls are deployed in our offices. Local firewalls are enabled on all laptops and desktops. Email (and attachments within) sent and received are scanned for malware by Mimecast before arriving at Office 365, which then undertakes further scanning.

Remote access is via a Citrix server. A SSL certificate is installed to ensure the connection from the user's machine to Citrix is secure.

From a management perspective we ensure our environment remains secure. Our systems are proactively monitored for potential issues and threats and we have a patch/update schedule for all hardware and software.

Only a small number of key individuals have named administrative accounts which are solely used for administrative tasks. All staff receive information security training as part of their induction and when they leave Churchill Hui their account is disabled immediately, and all equipment and data is returned to head office.

Rapport3: Churchill Hui's customer information database

Our main application is Rapport/Gekko, which acts as our customer information database and email archive store. Rapport and Gekko are cloud-based solutions hosted and managed by Cubic Interactive Ltd, who are responsible for the security of the platform. Cubic act as a data processor on our behalf and are registered with the Information Commissioner's Office (ICO), which means that they are already committed to delivering services in compliance with the current Data Protection Act and have also committed to comply with all the requirements of the GDPR.

Churchill Hui has named users within the system who gain access with an individual password and we have a policy requiring the use of complex passwords. As with our environment, when staff leave Churchill Hui, their account is disabled immediately.

Cubic's support and development centre holds Cyber Essentials security accreditation, and server access for Cubic Interactive staff is restricted and monitored. Access is IP restricted to only the Cubic offices and access to the website servers is audited. Passwords to these systems expire every 30 days and logins no longer needed are removed immediately.

The system is penetration tested on a regular basis and any actions raised are immediately processed by the relevant internal team or third party to ensure all known security risks are minimised.

Within the cloud-based services, Churchill Hui has a dedicated database stored on the Microsoft Azure platform which is secured to only allow access from the Rapport services and Cubic Interactive offices. This prevents any attempt to access this database outside of the provided software and support tools. The database makes use of advanced Microsoft Azure security functions such as Transparent Data Encryption to ensure data is stored in an encrypted format and Threat Detection

to monitor for malicious activity. The Rapport3 website is served over HTTPS with an SSL certificate to prove to the end user the site is genuine.

Currently the Rapport3 website is served from dedicated servers and hosted by Rackspace UK. This is monitored for malicious activity and hardware issues whilst being kept to a strict security standard covered by Rackspaces ISO accreditations (ISO27001 certificate is available upon request). Microsoft Azure and Rackspace internal traffic is monitored and managed by the relevant providers to ensure network integrity and operational security of the environment (further details are available directly from these suppliers).

Regarding support queries, maintenance and updates, Team Cubic is split into dedicated departments for each business function. Only staff members involved with support and commissioning work have access to our data, via a dedicated account. All support calls are comprehensively logged in a service desk tool and commissioning activities are carried out by a named account manager.

What is **personal information** used for?

Personal information is used in a business context for the purposes of contract delivery, such as contacting staff regarding projects, scheduling visits, accounts/payment, communication etc.

We may also email contacts with newsletters, event invitations or pertinent business information. These will always be relevant to our relationship with contacts, not infringe their freedoms and always include an straighforward way to opt-out of future communications.

Should a contact opt-out of communication this will be flagged on our system which will then prevent any subsequent marketing emails being sent. However, it will still allow emails regarding contract delivery or business critical information to be sent.

Finding out what we store about an **individual** or asking for information to be removed

At any time, an individual may ask to see what information we store about them (a Subject Access Request) and/or may ask for their personal information to be updated, transferred or removed from our systems (Right to be Forgotten). Any requests should be sent to london@churchill-hui.com, and we will action these.

Who is **data** shared with and why?

Personal information will only be shared with third parties when absolutely necessary for the purposes of contract delivery. For example, where a specific element of a project is undertaken by a sub-contracted third party.

Personal information is not shared, leased or sold to any third parties for marketing purposes.

How **data** is transmitted over email

We monitor all emails sent to us, including file attachments, for viruses or malicious software. Please be aware that you have a responsibility to ensure that any email you send is within the bounds of the law. We store emails for a minimum of 12 years following the conclusion of any appointment. Emails from Churchill Hui staff will be transmitted to fulfil a contract or prospective contract, legitimate business communications etc.

We take reasonable precautions to prevent the loss, theft, alteration or misuse of your personal information although we cannot guarantee or predict internet security.

We store all the personal information you provide on our secure servers. Office 365 uses Transport Layer Security (TLS) to encrypt the connection (not the email content) to the recipient's email server assuming this also supports TLS. If the receiving server doesn't support TLS the message will be sent insecurely.

For further information please call 020 8891 9191 or email london@churchill-hui.com.