Keybridge IT Solutions Ltd GDPR Statement

Commitment Statement

The EU General Data Protection Regulation (GDPR) is the most significant piece of European privacy legislation in recent history, replacing that of the 1995 EU Data Protection Directive (European Directive 95/46/EC). It aims to support the rights individuals have on data about themselves which is collected and stored. It also aims to detect, identify and mitigate against data breaches or leaks for all companies in the EU, as well as enforcing reporting on these issues. This aims to create one uniform policy across the EU regardless of whether the UK is part of the European Union. Any business that deals with EU nationals and business alongside their data must comply with the legislation.

Keybridge IT Solutions Ltd aims to comply with the applicable GDPR regulations as a data processor and controller. Working alongside its employees, clients and suppliers it will comply when the GDPR legislation takes effect on 25th May 2018.

Keybridge IT Solutions Ltd uses Third Party suppliers and software to process, control and manage data. These systems have been audited in line with GDPR commitments and outlined below. In the context of this statement, data subject refers to the person or entity submitting data and can include employees, clients and other individuals or organisations that **Keybridge IT Solutions Ltd** work with.

Data Collection

Keybridge IT Solutions Ltd collects potential customer information via meetings, marketing, public networking websites and exhibitions and similar opportunities / events. Data collection and processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract. The Contract a data subject enters, will entail **Keybridge IT Solutions Ltd** Terms and Conditions which are made available to them in both the signed contract, on the website and by request. By submitting data, the data subject agrees that this data can be processed and stored. We would obtain consent to process and store personal data including but not limited to; name, email and mobile number**. Keybridge IT Solutions Ltd** also requires information such as IP address and username and password in order to carry out the contractual obligations. **Keybridge IT Solutions Ltd** reserve the right to contact data subjects who have submitted this data both upon submission and in the future to ensure data is accurate.

Data Retention and Deletion

Keybridge IT Solutions Ltd delete customer data after a period of 7 years. Should any customer or employee of a Keybridge customer feel they wish to make a Subject Access Request (SAR), Data subjects must request their data by phone, email or letter stipulating what data they would like to access to, and this will be processed within 48 hours. We would send confirmation of this either by email or letter (whichever is most appropriate). If data has been deleted, erased or otherwise irretrievable the subject will also be informed of this.

Keybridge IT Solutions Ltd aims to keep data on file for a period of 7 years unless otherwise stipulated. Data would be hard erased after this time unless the subject of the data requests otherwise or has been engaged with during this time and data on them is necessary for archiving purposes in the public interest. Subjects of data have the right to be forgotten and erased from records upon request. Subjects must request their data by phone, email or letter stipulating what data they would like erased and this will be processed within 48 hours. We would send confirmation of this either by email or letter.

Data portability

The personal information **Keybridge IT Solutions Ltd** hold is limited to the contractual obligations and should any personal data be required to move to another provider, this would be made available in a suitable format.

Reporting data breach within Keybridge IT Solutions Ltd

As per the GDPR guidelines Keybridge IT Solutions Ltd must report a data breach within 72 hours after becoming aware of the breach, unless the breach itself is low risk. This is to be reported to the top authorities which would be ICO (Information Commissioner's Office) and the Data Protection Act Submission Form. This can be found here via this link or by using this security breach notification form (link here) or by reporting by phone on 0303 123 1113. Once a data breach or leak has been detected than it would be reported to this authority. A data breach or leak includes but is not limited to, a lost USB stick, loss or theft of portable devices or data sent to the wrong person**. Keybridge IT Solutions Ltd** is not responsible for monitoring and recording data breaches of its customers. The customer is the Data Controller and therefore responsible.

Internal Policies for GDPR

Keybridge IT Solutions Ltd execute a stringent security and access policy for employees that safeguards data and protects the integrity of data. The Company also ensure this doesn't impact business function and data subject or data subject experiences. **Keybridge IT Solutions Ltd** have a data security policy, confidentially policy, a password policy and a policy to target Bring Your Own Devices (BYOD) in the workplace. These policies aim to mitigate any instance of data breach or leaks and employees are trained in maintaining data security.

Keybridge IT Solutions Ltd use a number of cloud based systems in order to carry out their contractual obligations. These systems may hold customer information in the UK and Europe in secure data centres. To ensure customers information is safe, access to these systems are restricted to authorised personnel only and only accessed via Multi Factor Authentication, ensuring breaches are avoided as much as possible. Some of these systems enable trained **Keybridge IT Solutions Ltd** staff to remotely access a customer system. To ensure sensitive data is not seen without authorisation, the customer is asked in advance of an engineer connecting to their system. Further information relating to these policies ae found within the internal **Keybridge IT Solutions Ltd** GDPR Procedure Manual**.**

Keybridge IT Solutions Ltd do not hold customer data as this is stored on the customer's premises, or within another cloud system which is sold by Keybridge IT Solutions Ltd. Most commonly, email and files are stored within the **secure** Microsoft Cloud.

Keybridge IT Solutions Ltd CRMs and other Applications / Databases

Keybridge IT Solutions Ltd don't provide any business line applications or CRM systems and therefore the policies around data for these are the responsibility of the customer and / or the database manufacturer.

It is the customer's responsibility to determine what data is stored and processed, how long their data is stored for, to keep the data up to date and accurate and to ensure only required data is stored. **Keybridge IT Solutions Ltd** is here to assist with IT and GDPR where possible

This document is provided as of December 2017, for informational purposes to explain **Keybridge IT Solutions Ltd** stance on GDPR legislation and compliance. It is subject to change or removal without notice.

Keybridge IT Solutions Ltd - IT Systems and GDPR

Keybridge IT Solutions Ltd have strived to ensure customer's systems are best of breed and can align to GDPR. Below follows a summary of common systems supplied by **Keybridge IT Solutions Ltd** and information relating to how your data is stored and accessed, specifically in relation to the "Integrity and Confidentiality" principal of GDPR

System:	Keybridge Monitoring, Web Protection and Bit Defender AV
Primary Use:	For Network Monitoring, Computer updates, Anti-Virus, Firewall updates, system monitoring and IT Support
Storage and Security of Data	The systems are cloud hosted but do not contain personal information.
Backup	Backed up and encrypted to a number of UK Data Centres who have ISO 27001
Availability	Solarwinds offer a 99.99% SLA
Accessibility considerations	Keybridge Staff are trained to use these systems and in order to log in, have to use Multi Factor Authentication to prevent unauthorised access.

System:	Microsoft Office 365 / Azure
Primary Use:	Email, File Sharing & Collaboration / Virtual Servers and Cloud Storage
Storage and Security of Data	Stored securely within an ISO27001 accredited Data Centre in the UK. Replicated to other UK based Data Centres.
Backup	Data is backed up for 30 days by default and is encrypted.
Availability	Microsoft operates a 99.99% SLA
Accessibility considerations	Customer's staff can access this from anywhere using a valid Microsoft office 365 account. With EM+S you can use "multi factor authentication" to control who is logging in to your system. You can encrypt your documents and Emails, you can setup "single sign on SSO" to reduce number of passwords in circulation and you can also put controls in place to lock down where your systems can be accessed from. **Speak to Keybridge IT Solution if you wish to look in to these areas of additional security**
Subject Access Requests	Microsoft Office has a tool called eDiscovery that allows customers to quickly find all Information required within Emails, SharePoint and One Drive documents

System:	Keybridge File Backup
Primary Use:	Backup of Customer Data (typically from in house file and application servers)
Storage and Security of Data	Stored securely within an ISO27001 accredited Data Centre in the UK – London, Leeds and Manchester
Backup	Data is backed up for 30 to 365 days and is encrypted using 256bit AES encryption.
Availability	Backup servers are replicated across 3 data centres
Accessibility considerations	Authorised Keybridge staff can access this data for backup / restore purposes. Access can be restricted to certain IP addresses for further security

Keybridge IT Solutions™

IT considerations by System / Service

System / Service	Overview and Recommendations
Network	Customer's networks are monitored for Viruses and for updates by the Keybridge NOC (Network Operations Centre). Internal LANs are protected by Keybridge Anti Virus and by customer's firewall. Breaches can be detected by Server or Network audit logs **Recommendations**: • Strong Passwords to prevent unauthorised access • Staff awareness of security, e.g. not to write down passwords – this should be part of the customer's password policy • Consider Locking down any remote access to the corporate network if not already done • Microsoft Threat Analysis tools – this is a product within the Microsoft EM+S suite and is installed locally to actively monitor breaches
PCs, Laptops and Mobile devices	Customer's Computers are monitored for Viruses and for updates by the Keybridge NOC (Network Operations Centre). Internal LANs are protected by Keybridge Anti Virus and by customer's firewall. Breaches can be detected by local windows Security Logs **Recommendations**: • Strong Passwords to prevent unauthorised access • Staff awareness of security, e.g. not to write down passwords – this should be part of the customer's password policy • Keybridge Web Protection to further protect against Malware and other kind of threats • Do not allow remote access to PCs and Laptops • If you don't have a server, have all computers configured to join to "Azure AD" – this means staff log in to their PCs with their Office 365 credentials • Using EM+S, encrypt all PCs and Laptops

Emails and Documents	Keybridge recommends customers to use Office 365. (95% of our customers use this). The systems are protected by licensed accounts. **Recommendations**: • Customer's staff can access this from anywhere using a valid Microsoft office 365 account. With EM+S you can use "multi factor authentication" to control who is logging in to your system. You can encrypt your documents and Emails, you can setup "single sign on SSO" to reduce number of passwords in circulation and you can also put controls in place to lock down where your systems can be accessed from. • Become familiar with eDiscovery to help with Subject Access Requests