GDPR Customer & Partner Addendum

GDPR - YOUR CONTRACT WITH SAPPHIRE SYSTEMS LIMITED

As an existing customer or partner of Sapphire Systems Limited, it is important that you read the information below regarding changes to your existing contract with us to accommodate the General Data Protection Regulation (GDPR).

The data protection legislation aims to protect the privacy of all EU citizens and prevent any data breaches of EU citizens' personal data. It will apply to any public or private organisation processing personal data.
This document is our 'Data Protection Addendum' (which is based on the Sapphire Standard Terms and Conditions). For the avoidance of doubt, the term 'Customer' within the Addendum refers to both customers and partners of Sapphire.

We have provided additional resources around GDPR to comply with our GDPR obligations, including additional security and organisation process measures.

We kindly request you to forward this communication along with the enclosed Data Protection Addendum to an authorised signatory for your company.

Any queries, please email: GDPR.enquiries@sapphiresystems.com

Sincerely,
Sapphire Systems Limited

ADDENDUM TO IMPLEMENT LEGISLATIVE OBLIGATIONS RELATING TO DATA PROCESSING OF PERSONAL DATA AND DATA SUBJECTS

This Addendum is entered into on the date of signature of the last party hereto and is supplemental to all terms and conditions currently in place between the Customer and SAPPHIRE but replaces any provision relating to the processing of Personal Data by SAPPHIRE.

1.1 IT IS HEREBY AGREED AS FOLLOWS:

1. The following definitions will apply:

"Parties" means the contracting parties set out in the Agreement;

"Applicable Law" means the laws of England and Wales (and any EU regulations from time-to-time applicable (i) whilst the United Kingdom remains a member of the European Union or (ii) subsequently under the terms of the European Union (Withdrawal) Bill);

"Controller" has the meaning set out in the Data Protection Legislation;

"Customer" means the contracting party, which is not Sapphire, set out in the signature block at the end of this Addendum;

"Data Loss Event" means any event that results, or may result, in unauthorised access to Personal Data held by Sapphire hereunder, and/or actual or potential loss and/or destruction of Personal Data in breach of the Clauses contained in this Addendum, including any Personal Data Breach;

"Data Protection Legislation" means all applicable privacy or data protection laws and regulations (as amended, consolidated or re-enacted from time-to-time) that relate to the protection of individuals with regards to the processing of personal data to which a party is

subject, including the Data Protection Act 1998 (as may be superseded) and GDPR for as long as any of the above are incorporated into Applicable Law together with any guidance and/or codes of practice issued from time-to-time by the Information Commissioner;

"Data Subject" has the meaning set out in the Data Protection Legislation;

"Data Subject Access Request" means a request made by, or on behalf of, a Data Subject in accordance with rights granted under the Data Protection Legislation to access their Personal Data;

"EEA" means the European Economic Area;

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and repealing Directive 95/46/EC (General Data Protection Regulation);

"Agreement" the Sapphire Standard Terms and Conditions currently in force between the Parties;

"Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed;

"Processor" means a natural or legal person or any other body which processes personal data on behalf of the controller;

"Security Measures" means appropriate technical and organisational measures which are set out in the service description (or other relevant documentation available) for the relevant products or services provided by the Processor;

"Sub-processor" means any third party appointed to process Personal Data on behalf of SAPPHIRE related to the Agreement when and if applicable.

2. Notwithstanding any provisions in the Agreement relating to the protection of individuals with regards to the processing of Personal Data, such provisions will be superseded in their entirety and replaced by the following clauses.

3. The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and SAPPHIRE is the Processor.

4. SAPPHIRE shall notify the Customer immediately if it considers that any of the Customer's instructions infringe the Data Protection Legislation.

5. SAPPHIRE shall provide reasonable assistance to the Customer in relation to compliance with the Data Protection Legislation.

6. SAPPHIRE shall, in relation to any Personal Data processed in connection with its obligations to the Customer:

6.1 promptly notify the Customer before processing the Personal Data unless prohibited by Applicable Law;

6.2 ensure that it has Security Measures in place (available on request) and the Customer hereby confirms that such Security Measures are appropriate to protect against a Data Loss Event having taken into account the nature of the Personal Data to be protected; harm that might result from a Data Loss Event; state of technological development; and cost of implementing any additional measures;

6.3 In relation to the clauses above, the Controller is responsible (as between the parties and to Data Subjects and supervisory authorities) for:

6.3.1 Ensuring that Data Subjects have given appropriate consent to the processing of any Personal Data by the Processor;

6.3.2 Ensuring that the Security Measures meet the GDPR standard of appropriateness;

6.3.3 Claims or complaints resulting from SAPPHIRE's actions to the extent that such actions directly result from instructions received from the Customer.

6.4 In relation to 7.3.2, the Parties acknowledge that the Processor may not be in a position to assess what measures are appropriate to the Controller's Personal Data (since the data is collected and processed for the Controller's and not the Processor's business). The Controller may, therefore, select chargeable services for additional security measures which exceed the standard security measures provided by the Processor to ensure that Sapphire Personnel:

6.4.1 does not process Personal Data except in accordance with this clause 7; and;

6.4.2 it will take all reasonable steps to ensure the reliability and integrity of any Sapphire or third party personnel who have access to the Personal Data and ensure that they:

i. are aware of and comply with Sapphire's duties under this clause;

ii. are subject to appropriate confidentiality undertakings with Sapphire or any Sub-processor (whether and if applicable);

iii. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Customer or as otherwise permitted hereunder; and

iv. have undergone adequate training in the use, care, protection, and handling of Personal Data; and

v. does not transfer Personal Data outside of the EEA unless the prior written consent of the Customer has been obtained and the following conditions are fulfilled:

a) the Customer or SAPPHIRE has provided appropriate safeguards in relation to the transfer (in accordance with GDPR Article 46) as determined by the Customer;

b) the Data Subject has enforceable rights and effective legal remedies;

c) Sapphire complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses all reasonable endeavours to assist the Customer in meeting its obligations); and

d) Sapphire complies with any reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data;

7. The Customer also agrees that given the nature of the service, SAPPHIRE will be able to have access to Customer's personal data from outside the EEA.

8. SAPPHIRE upon written request of the Customer, will delete or return Personal Data (and any copies of it) to the Customer on termination unless SAPPHIRE is required by Applicable Law to retain the Personal Data.

9. Before allowing any Sub-processor to process any Personal Data related hereto SAPPHIRE must give the Customer:

9.1 At least 30 calendar days' notice in writing of the intended Sub-processor and processing;

9.2 confirmation that there is a written agreement with the Sub-processor which give effect to the terms set out in this clause 10 such that they apply to the Sub-processor

9.3 such information regarding the Sub-processor as the Customer may subsequently reasonably require.

10. SAPPHIRE shall remain fully liable for all acts or omissions of any Sub-processor (when and if applicable).

11. Subject to clause 7, SAPPHIRE shall notify the Customer immediately if it:

a) receives a Data Subject Access Request (or purported Data Subject Access Request) relevant to the Customer;

b) receives a request to rectify, block or erase any Personal Data relevant to the Customer;

c) receives any other request, complaint, or communication relating to either party's obligations under the Data Protection Legislation;

d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data, relevant to the Customer, processed hereunder

e) receives a request from any third party relevant to the Customer for disclosure of Personal Data where compliance with such request is required or purported to be required by Applicable Law; or

f) becomes aware of a Data Loss Event relevant to the Customer.

12. SAPPHIRE's obligation to notify under clause 12 shall include the provision of further information to the Customer, as details become available.

13. Taking into account the nature of the processing, SAPPHIRE shall provide the Customer with full assistance in relation to either Party's obligations under Data Protection

14. Legislation and any complaint, communication, or request made under clause 12 (within the timescales agreed between the Parties) including by promptly providing:

a) the Customer with full details and copies of the complaint, communication, or request;

b) such assistance as is reasonably requested by the Customer to enable the Customer to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

c) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data, relevant to the Customer, processed hereunder;

d) receives a request from any third party relevant to the Customer for disclosure of Personal Data where compliance with such request is required or purported to be required by Applicable Law;

e) becomes aware of a Data Loss Event relevant to the Customer.

15. SAPPHIRE shall maintain complete and accurate records and information to demonstrate its compliance with Article 30 of GDPR.

16. SAPPHIRE shall allow for audits of its security measures and data processing activities by the Customer or the Customer's designated auditor at reasonable times and on reasonable notice.

17. For the avoidance of doubt, notwithstanding anything to the contrary in the Agreement, each party accepts liability for loss of Personal Data to the extent that the loss of Personal Data is caused by:

- a material breach by such party of their data processing obligations under Applicable Law
- a failure by such party to provide the Security Measures that it was contractually committed to providing concerning such Personal Data will be fined up to the sum of £1,000,000.

18. Notwithstanding anything to the contrary set out in the Agreement, to the extent that there is any duplication or conflict between definitions or clauses used in the Agreement and this Addendum, the definitions and clauses set out in this Addendum will apply and take precedence. In all other respects, the Agreement as amended by this Addendum shall continue in full force and effect.

19. Each Party confirms that their signatory set out below is a duly authorised representative and authorised to act on behalf of the relevant party.

20. This Addendum is governed by the laws of England and Wales and the parties submit to the exclusive jurisdiction of the courts of England and Wales.

SAPPHIRE SYSTEMS GDPR – FREQUENTLY ASKED QUESTIONS

PROCESSES, POLICIES & PROCEDURES

1.	**Does Sapphire have a dedicated individual(s) responsible for data protection and/or information security?** Yes. There are several individuals in our organisation that are responsible for security. The principal team is our Technical department. Our Technical team manages our internal security and system security. It also performs technical services on behalf of our customers. In addition, we have a Technical Manager that secures, implements security applications, and ensures that security processes are compliant and adopted across the business.
2.	**Does your organisation have privacy/ data protection /information security policies in force?** Due to the high level of security throughout our company, we are certified with an ISO 27001 certification.
3.	**Is there a published version of these policies available?** The majority of our policies are published via our company website. For those that are not available online, a copy can be provided on request.

4	How often does your organisation review and update any policies and procedures? To ensure that our documentation and processes reflect any changes that may occur, we review and update our policies and procedures often. This review occurs annually at the very least.
5.	Is there a register of subject access requests? Yes. These requests are managed per department and registered with our HR department.
6.	Do you have a well-defined staff leaver's process in place to ensure that all access to a terminated employee is revoked? Yes. A leavers' notification is sent out promptly to the team leaders of each department in order to ensure all access is revoked no later than the termination date.
7.	Should someone like to exercise their right of erasure, how soon will this request be carried out? Can you delete or amend any personal data on request and what is your timeframe? Our organisation prides itself on knowing where all of its data is stored. The turnaround for deletion or amendment can be achieved quickly - 48 hours to 28 days.

8.	How soon is customer data removed from your system(s) following the termination of service? This timeframe is dependent on the customer's contract, however, we can achieve a termination on our system(s) between 48 hours to 28 days.

TRAINING AND SECURITY

1.	Do you have any security accreditation in place? Yes. Sapphire is ISO 27001 and ITIL certified.
2.	Do you have a secure network architecture in place? Yes, the architecture of our data centre network is securely provisioned and administered with controlled ingress and egress points. Our external connectivity is also encrypted.
3.	Do you have a clear desk policy that protects Critical National Infrastructure/ Computer Network Defence (CNI/CND) against unauthorised access, loss, or disclosure arising from data stored on USB devices or printed media? Yes, we do as this is part of the ISO27001:2013 standard principles.

4.	**Is there an acceptable usage policy that states that all personnel is required to understand and comply with their responsibilities regarding the acceptable use of the organisations messaging systems (including email and instant messaging), internet and telephone facilities, which are provided for business purposes?** Yes, we do. Employees are required to take regular ISO awareness briefings classes. We also enforce that this class is taken on a new employee's day of induction.
5.	**What data protection and/or information security training is provided within your organisation?** All new employees receive ISO 27001 compliant data and security training when joining our organisation. These sessions are conducted by HR and the IT department and comprise of system access and data security protocols, we also document this information in our HR manuals.
6.	**How do you ensure that the equipment and systems used to provide a service are not accessed by unauthorised users?** We have a security access process in place that assigns rights based on need and to approved users - Role-Based Access Control (RBAC).

7.	Does Sapphire maintain a register of data breaches? To accurately log events that have occurred, we always keep a register of any data breach, no matter the scale. To date, we can say that we have not been breached.
8.	How would Sapphire know whether it had been the object of a data breach? We have intuitive alerts that are activated via our firewall software, CrowdStrike. Once an alert is triggered, these alerts are sent to our technical team, irrespective of where they are, and managed promptly. With this in place, we are sure to adhere to the 72 hours deadline set by GDPR to notify customers and the Information Commissioner's Office (ICO) about a possible breach.

9.	In what timescale are data breaches reported to customers? Sapphire endeavour to report any breach of a customer's data within 4 hours of awareness and subsequent investigations.
10	Do Sapphire perform security/penetration testing and how often do they occur? Yes, we do perform security and penetration tests and we carry them out annually.

11.	**Are technical measures taken to restrict access to systems that hold personal, confidential, or sensitive data?** We ensure that all of our personnel have password-protected access to our systems and depending on the type of data and the system, the access is controlled further to only allow a small percentage of staff access and in some cases for a limited period. In addition, we also enforce strong password complexity and implement an account lockout mechanisms.
12.	**How do sapphire enforce security policies and who is responsible for ensuring that these security policies are adhered to?** Our Chief Information Officer (CIO) and Global IT and Technical Manager oversee all of our security policies.
13.	**What security software do you use?** We understand that with security you can never be too careful and due to this, we have achieved our ISO 27001 because we have taken several measures to ensure that our security and the security of our customers is protected to the highest of standards. To attain this, we use the following software: **CrowdStrike** - Endpoint sensor to detect ransomware **Symantec** - Protection against advanced threats, malware, and other cyber attacks. **Qualys** - Auditing, compliance, and protection of our IT systems and web applications **AppCheck NG** - Vulnerability scanning.

14.	How often is access to written or printed material and access to computer systems reviewed? Access to our systems is reviewed, in some cases, daily. In a majority of instances, it is reviewed monthly in compliance with the ISO27001.
15.	What is your organisation's process for the disposal of the computer equipment used in processing data? Any printed personal customer data is securely shredded or placed in confidential waste bins. Any electrical equipment is returned to our IT department for a secure wipe and/or disposal.
16.	After a security advisory has been issued, how soon does Sapphire offer a patch release? We schedule patch releases every 6 months once they have been tested and compatibility has been assured via our User Acceptance Testing (UAT) system. If a security advisory has been issued, we would accelerate a patch release in line with the supplier's advice.

17.	**Who conducts your security audits and what is covered in your security audits?** Sapphire conducts its own internal penetration tests and authorises security audits for our customers upon their request. These security audits cover identifying vulnerabilities in security by scanning, reviewing application and operating system access controls, analysing physical access to the systems and correcting any known issues and bugs.
18.	**Would you be willing to allow us to security test your service?** Yes. Any time required from Sapphire consultants and technicians is chargeable on a time and materials basis during any such exercise.

SERVICE RESILIENCE AND CONTINUITY

1.	**Where do Sapphire store their backups and how long is customer data retained?** Sapphire's backup data is stored in two data centres. These datacentres are located in Greenwich, London, and Birmingham within the United Kingdom. The timeframe that data is retained for is dependent on the contract of the customer. Customer data that has been backed up and is used for support purposes or where Sapphire is managing the customer's infrastructure via our Sapphire Anywhere service, is held for the time stipulated by the contract. This is to ensure that the duties required can be successfully completed and can, in some cases, range from a week to a year. The daily processing of backups created whilst we deliver our Sapphire Anywhere service is usually held for 14 days before auto-deletion
2.	**Do you replicate data to an alternate location?** All our data stores are replicated every day via Windows Hyper-V replication in line with ISO27001.
3.	**Does Sapphire have any controls are in place to ensure that encryption keys are safely secured?** To ensure that our encryption keys are safe and secure we use ManageEngine Key Manager. This is a web-based key management solution that helps consolidate, control, manage, monitor, and audit the entire life cycle of SSH (Secure Shell) keys and SSL (Secure Sockets Layer) certificates.

SUB-PROCESSING

1.	**Does Sapphire outsource, at any stage and to any extent, any personal data processing?** We do not outsource any data processing to external companies. We have highly skilled staff that are proficient in every aspect of processing our client data.
2.	**Does Sapphire use standard data protection contractual clauses in your relationship with third-party service providers and third-party data controllers?** Yes. We have a legally binding Non Disclosure Agreement (NDA).
3.	**Do you maintain a register of third-party data processors to whom you transfer personal data?** We seldom transfer any data to any third party. Should we do this, we will always keep a log of the company, date, time, and any additional key information as a reference. We also request approval from authorised personnel, usually a CFO or CTO in the form of a signed company letter indicating who has access, what access should be granted, and for how long access is required.

4.	What provisions are in place to ensure the integrity and confidentiality of any subcontractors/consultants you hire? Less than 5% of our services are undertaken by contractors – that is our policy. In the case that a contractor is required, we would ensure that a signed contractual agreement is in place. This is all in compliance with Sapphire's ISO27001 protocol.

View a copy of our Sapphire Privacy and GDPR Compliance policy Here