SCHEDULE 3.9 – DATA PROTECTION FOR MICROSOFT 365

1. APPLICATION

1.1 This schedule, which contains a description of the Data Protection Product, forms part of the Agreement entered into between the Parties for the provision of the Services.

1.2 By accepting an Order or by installing, accessing or using the Services you acknowledge and agree to these terms and conditions and the General Conditions. If you do not agree to these terms and conditions you must not use the Services.

1.3 Definitions and interpretations that are specific to this Schedule 3.9 are set out in **Annex 1** and apply in addition to the definitions and interpretations set out in **Schedule 1 (Definitions)** of the General Conditions.

2. SERVICE DESCRIPTION

2.1 The Customer will receive the current standard Data Protection Product features and functionality (such as number and frequency of back-ups or retention schedule) for the number of Users and/or data allotment as specified in the Order.

2.2 The Customer represents and warrants that the Supplier is acting as an agent on behalf of the Customer and confirms that the Supplier has full authority to agree to the terms and conditions in this Schedule 3.9 with its Third-Party Supplier in respect to access, use and support by the Third-Party Supplier of the Data Protection Product and Backed Up Data.

3. CUSTOMER OBLIGATIONS

3.1 The Customer is responsible for the security of all the Customer's access credentials to the Data Protection Product, including any action the Customer permits any person or entity to take related to the Data Protection Product and Backed-Up Data using the Customer's access credentials.

3.2 The Customer is responsible for the proper configuration and maintenance of safeguards as they relate to access to and use of the Data Protection Product and Backed-Up Data, including but not limited to individual Administrator and User permissions, local Device access, network connectivity and internet connectivity.

3.3 The Customer agrees to notify the Supplier as soon as practicable of any unauthorised use of any access credentials, password or account or any other known or suspected breach of security.

3.4 The Customer may not nor permit, facilitate or authorise any third party to:

3.4.1 use the Data Protection Product other than as permitted under this Schedule 3.9;

3.4.2 remove or destroy any copyright or other proprietary markings for the Data Protection Product or its Specifications;

3.4.3 access or use the Data Protection Product in any manner that could damage, disable, or overburden such Data Protection Product, any networks or security systems;

3.4.4 reverse engineer, decompile, disassemble, or otherwise attempt to extract source code from the Data Protection Product, except to the extent this restriction is expressly prohibited by Applicable Law;

3.4.5 copy, modify or create derivative works of the Data Protection Product;

3.4.6 alter any disabling mechanism which may reside in the Data Protection Product;

3.4.7 assign, sublicense, rent, timeshare, loan, pledge, lease, or otherwise transfer the Data Protection Product, or directly or indirectly permit any unauthorized party to use or copy the Data Protection Product;

3.4.8 conduct or disclose the results of any form of benchmarking of the Data Protection Product;

3.4.9 extract any software for use in other applications; or

3.4.10 access the Data Protection Product to (i) build a competitive product or service; (ii) copy any, or build a product using, ideas, features or graphics sourced from the Data Protection Product.

3.5 Use of the Data Protection Product and Backed-Up Data must at all times be in compliance with all Applicable Laws.

3.6 The Data Protection Product and Backed-Up Data may not;

3.6.1 be used to send any unsolicited commercial email or invitation in violation of Applicable Law;

3.6.2 be used to process or disclose any unencrypted personally identifiable data (such as payment card numbers or social security numbers) in violation of any Applicable Law;

3.6.3 be deceptive, fraudulent, harmful, abusive, harassing, threatening, indecent, obscene, racially, ethnically, or otherwise objectionable, hateful, tortious, libellous, defamatory, slanderous, or otherwise in violation of Applicable Law;

3.6.4 infringe or misappropriate any Intellectual Property Rights or other rights of any third party;

3.6.5 be used to transmit any viruses or similar malicious software that may damage the operation of any computer, network, system or the Products; or

3.6.6 violate the terms of use of the Backed-Up Site or any other agreement.

3.7 If the Supplier reasonably believe the Data Protection Product use or Backed-Up Data:

3.7.1 violates any of the restrictions in the foregoing paragraphs;

3.7.2 may disrupt or threaten the operation or security of any computer, network, system or the Data Protection Products; or

3.7.3 may otherwise subject the Supplier to liability

the Supplier reserves the right to refuse or disable access to the Data Protection Product and/or Backed-Up Data. The Supplier may also take such action as required to comply with Applicable Law. The Supplier will use reasonable efforts to contact the Customer prior to taking such action. However, the Supplier may restrict access to the Data Protection Product or Backed-Up Data without prior notice as necessary to comply with Applicable Law or to protect against damage or security threats. If the Supplier takes any such action without prior notice, the Supplier will later provide notice to the Customer, unless prohibited by Applicable Law.

4. SERVICE CONDITIONS

USE OF DATA PROTECTION PRODUCT

4.1 Subject to the terms and conditions in this Schedule 3.9 and receipt by the Supplier of all Charges applicable to the Data Protection Product, the Supplier hereby grants a limited, revocable, non-sublicensable, non-exclusive right to access and use the Data Protection Product during the Minimum Term and Successive Terms for the number of Users and /or

the applicable data storage allotment set forth in an Order. The Data Protection Product can only be used for internal business purposes and not for further resale or distribution.

4.2 The Data Protection Product is licensed, not sold. The Data Protection Product contains material that is protected by copyright, patent and trade secret law of jurisdictions throughout the world, and by international treaty provisions. Except for the limited rights granted in this Schedule 3.9, the Third-Party Licensor retains all rights, title, interest and Intellectual Property Rights in the Data Protection Product.

4.3 The Third-Party Licensor reserves the right at any time to make Enhancements to, replace, modify, discontinue or add to the Data Protection Product, including revisions to Specifications, features and functionality. The Supplier will use reasonable commercial efforts to provide the Customer notice of any material changes by updating relevant information in the applicable Online Portal.

4.4 The Third-Party Licensor may designate enhancements to the Data Protection Product or a new Data Protection Product as "Beta Product" that the Supplier may make available. Such Beta Product will not be ready for use in a production environment and its operation may be unpredictable and lead to erroneous results. The Customer is under no obligation to use a Beta Product.

4.5 Where the Customer chooses to use a Beta Product, the Customer agrees that the Beta Product;

4.5.1 is experimental and has not been fully tested;

4.5.2 may not meet the Customer's requirements;

4.5.3 use or operation may not be uninterrupted or error free and is for purposes of evaluating and testing the product and providing feedback to the Third Party Supplier.

4.6 The Customer agrees to report promptly to the Supplier any errors or other deficiencies in the Beta Product and will hold all information relating to use and performance of the Beta Product in strict confidence and not disclose such information to any unauthorised third parties.

4.7 Use of any Beta Product is otherwise subject to this Schedule 3.9. NOTWITHSTANDING ANY OTHER PROVISION OF THESE TERMS OF USE, ALL BETA PRODUCT IS PROVIDED "AS-IS" AND "AS-AVAILABLE," WITHOUT WARRANTIES OF ANY KIND. The Customer hereby waivers all claims, now known or later discovered, that the Customer may have against the Supplier and its Third Party Suppliers and licensors arising out of use of any Beta Product.

4.8 The Data Protection Product may be configured to designate the geographic region where Backed-Up Data associated with the Data Protection Product is stored. The European Data Processing Addendum is incorporated into this Schedule 3.9 where the Data Protection Product is configured to store Backed-Up Data in the European Economic Area.

BACKED-UP DATA

4.9 The Customer represents and warrants it has all rights (including from Backed-Up Sites and Users) as necessary to permit access, copying and use of Backed-Up Data with the Data Protection Product.

4.10 The Customer is responsible for the accuracy, quality and legality of the Backed-Up Data, and the means by which the Customer acquired rights to the Backed-Up Data for use with the Data Protection Product. For purposes of this Schedule, Backed-Up Data is the property of Customer, not any User, and the Supplier is under no obligation to inform Users that the Customer controls such information with the Supplier.

4.11 The Customer, for itself and its Users, authorises the Supplier and its Third Party Supplier to access and interact with the Backed-Up Site to retrieve Backed-Up Data and grants the Supplier and its Third Party Supplier a limited, royalty-free, non-exclusive, assignable license to use, copy, reformat, display, disclose and distribute the Backed-Up Data solely for providing the Data Protection Product as described in this Schedule, including as authorised by an Administrator for support, and as described in the Third Party Supplier's Privacy Policy.

4.12 The Customer retains all its right, title and interest in and to the Backed-Up Data, and the Supplier and Third Party Supplier neither own nor acquire rights in the Backed-Up Data other than the rights expressly granted under this Schedule.

4.13 The Supplier and Third-Party Supplier will use physical, technical and administrative safeguards, consistent with commercially reasonable industry practices, designed to secure the confidentiality, integrity and availability of Backed-Up Data under its control against accidental or unauthorized loss, access or disclosure.

4.14 The Supplier and Third-Party Supplier will use the same safeguards for all Backed-Up Data, regardless of its nature or contents. The Supplier and Third-Party Supplier are both a Processor and not a Controller of all Backed-Up Data.

4.15 The Customer must maintain authorisation and access to the Backed-Up Sites so that the Supplier and Third- Party Supplier is regularly able to access Backed-Up Data for purposes of providing the Data Protection Product.

4.16 The Customer agrees and acknowledges that Backed-Up Data may not be available or restorable;

4.16.1 if the Customer changes such access authority or otherwise restricts the Supplier's and/or the Third Party Supplier's access to such Backed-Up Site;

4.16.2 due to unavailability of the Backed-Up Site; or

4.16.3 with respect to modifications to the Backed-Up Data that are not captured in the backup frequency or retention schedule for the Data Protection Product.

4.17 Unless otherwise agreed to in writing by the Supplier, the Customer agrees that Backed-up Data will not contain Special Category Data. If the Backed-Up Data does include Special Category Data, the Customer shall indemnify the Supplier for all losses, damages, costs,, expenses or other liabilities incurred by, awarded against or agreed to be paid by the Supplier arising from, or in connection with the Processing of the Special Category Data. The Customer further acknowledges that the limitation of liability provisions contained in this Schedule and the General Conditions shall not apply to the indemnity in this paragraph 4.17 and as such the Customer's liability to the Supplier shall be unlimited.

USE OF OTHER INFORMATION

4.18 If the Customer provides the Supplier or Third Party Supplier with comments or other feedback regarding the Data Protection Product or the their business (collectively "**Feedback**"), directly or through any third party, the Customer does so without any expectation of compensation and hereby grant the Supplier and its Third Party Supplier a worldwide, irrevocable, perpetual, royalty-free right and license to use the Feedback to improve the Data Protection Product and for any other purpose. Feedback is strictly voluntary, and the Supplier is not required to hold it in confidence.

4.19 Notwithstanding anything else in this Schedule or otherwise, the Supplier and Third-Party Supplier may evaluate, and process use of the Data Protection Product and Backed-Up Data in an aggregate and anonymous manner and compile related statistical and performance information ("**Aggregate Data**").

4.20 The Supplier and Third-Party Supplier may use and share such Aggregate Data to improve the Data Protection Product, develop new products, analyse usage, and generally for any purpose related to the Supplier's business. The Supplier and Third-Party Supplier will retain all Intellectual Property Rights in Aggregate Data. For clarity, Aggregate Data does not include personally identifiable information or information that can identify any natural person.

4.21 Operational data concerning use of the Data Protection Product ("**Log Data**"), that servers automatically record relating to the access and use of the Data Protection Product, IP address, authentication tokens, machine identification, access logs, and settings are used by the Supplier and the Third-Party Supplier to provide the Data Protection Product and operate its business and the Customer agrees that the Supplier and Third-Party Supplier may use such Log Data for such purposes.

SUPPORT SERVICES

4.22 The Supplier will assist the Customer with set up of the Data Protection Product by providing access to the Online Portal and undertaking the initial set up of the Back Up Schedule. The Supplier will also provide the Customer with documentation comprising instructions for use of the Data Protection Product. Unless the Customer purchases Support Services from the Supplier, the support provided to the Customer is limited to that described in this paragraph 4.22.

4.23 Where the Supplier provides the Customer with Support Services in relation to the Data Protection Product the Support Service shall be provided in accordance with **Schedule 4.4 (Managed Support Services)**.

4.24 Where the Supplier provides the Customer with Professional Services in relation to the Data Protection Product, the Professional Services shall be provided in accordance with **Schedule 4.2 (Professional Services**).

4.25 The Customer authorises the Supplier, and where applicable the Third-Party Supplier, to access the Data Protection Product and/or the Backed-Up Data in order for the Supplier to provide support pursuant to paragraph 4.21 above, **Schedule 4.2 (Professional Services)** or **Schedule 4.4 (Managed Support Services).** The Supplier may rely on the instructions and authorisations given to us by any Administrator with access to the Data Protection Product, and we will have no obligation to inform any other Administrator of the same.

4.26 The Customer authorises the Suppler and the Third-Party Supplier to interact remotely with any deployed Data Protection Product in order to test, troubleshoot, or update it as required from time to time. During maintenance windows the Data Protection Product may not be accessible. The Supplier will make reasonable efforts to notify the Customer of such maintenance windows.

5. CHARGES AND PAYMENT

5.1 This paragraph 5 is supplemental to clause 6 of the General Conditions and in the event this paragraph 5 conflicts with clause 6 of the General Conditions, this paragraph shall take precedence.

5.2 The Supplier shall invoice the Customer the Charges for the Data Protection Product as set out in paragraph 5.3 in the amounts specified in the Order.

5.3 Unless stated otherwise in the applicable Order, the Supplier shall invoice the Customer as follows:

5.3.1 Set Up Charges on or after the Commencement Date;

5.3.2 License Fees monthly in arrears; and

5.3.3 Termination Charges upon termination of service and / or the Agreement.

Herein after defined "**the Charges**".

5.4 Where the Data Protection Product is provisioned after the 15th of the month, the Customer will be charged License Fees from the 1st of the following month. In such circumstances the Commencement Date as defined in the General Conditions shall be deemed amended to the 1st of the following month for the purposes of calculating the Minimum Term.

5.5 The Supplier will charge the Customer for any Support Services in accordance with the relevant Schedule 4.

6. TERM AND TERMINATION

6.1 This paragraph 6 is supplemental to clause 2 and 8 of the General Conditions and in the event this paragraph 6 conflicts with clause 2 and 8 of the General Conditions, this paragraph shall take precedence.

6.2 This Agreement shall commence on the date of this Agreement and shall continue in force for a minimum period of 12 twelve (12) months from the Commencement Date or as otherwise specified in the applicable Order ("**Minimum Term**") and thereafter shall be renewed automatically for successive periods of twelve (12) months (each a "**Successive Period")** unless terminated:

6.2.1 by the Customer giving the Supplier not more than ninety (90) days and no less than thirty (30) days written notice, before the end of the Minimum Term or Successive Term;

6.2.2 in accordance with clause 8 of the General Conditions; or

6.2.3 in accordance with this Schedule 3.9.

6.3 The Customer acknowledges and agrees that the Supplier will automatically provision a license for the Data Protection Product for every new Microsoft User which is added to the Customer's Microsoft account. Where a license for the Data Protection Product is automatically provisioned, the license(s) shall be coterminous with the Minimum Term of the licenses provided in the initial Order placed by the Customer for the Data Protection Product. All licenses for the Data Protection Product will therefore expire on the same date.

6.4 If the Customer does not wish for a license to be automatically provisioned for an additional User in accordance with paragraph 6.3 above, then it must notify the Supplier in advance of the User being added to the Customer's Microsoft account.

6.5 The Customer acknowledges and agrees that where a User is removed from the Customer's Microsoft account, the relevant license for the Data Protection Product will not automatically be removed or terminated but rather it will continue to be provided unless and until the relevant license is terminated by the Customer in accordance with the terms of the Agreement.

6.6 The Customer may cancel licenses during the Minimum Term giving not less than thirty (30) days written notice to expire the on the last day of the month. The Customer will not be liable

to pay Termination Charges for such licenses provided the number of licenses remains the same or higher than the number of licenses in the initial Order placed by the Customer for the Data Protection Product.

6.7 If a Backed-Up Site amends its API guidelines in such a way that materially affects the Supplier's or Third Party Supplier's ability to access the Backed-Up Site to provide the Data Protection Product in accordance with the Specifications, and if the Supplier and Third Party Supplier is unable to perform substantially the same functionality, either party may terminate the applicable Order by providing to the other thirty (30) days' written notice.

6.8 Upon any termination of the Agreement or Services (as applicable), the Customer will immediately discontinue all use of the Data Protection Product.

6.9 For up to sixty (60) days after the effective date of termination, the Supplier will, upon written request allow the Customer to export or download a copy of its Backed-Up Data as provided in the Specifications. After such period, the Supplier has no obligation to maintain or provide any Backed-Up Data and may thereafter delete or destroy all copies of the Backed-Up Data, unless legally prohibited.

6.10 Subject to paragraph 6.6 and 6.7 above, the Customer shall be liable to pay Termination Charges to the Supplier in accordance with clause 8.7 of the General Conditions where the Agreement or any Services are terminated within the Minimum Term of Successive Term.

7. LIABILITY

7.1 This paragraph 7 is supplemental to clause 9 of the General Conditions and in the event this paragraph conflicts with clause 9 of the General Conditions, this paragraph shall take precedence.

7.2 During the Subscription Term, we will provide the Data Protection Product using a commercially reasonable level of skill and care in material accordance with the available Specifications. The Customer's sole and exclusive remedy in the event that the Supplier does not do so shall be to terminate the Agreement 8.1.1 of the General Conditions.

7.3 Except for the limited warranties herein, the Data Protection Product is provided as is and with all faults. To the maximum extent permitted by Applicable Law, the Supplier does not provide any promise, representation or warranty, whether express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, system integration, data security, or warranties arising out of any course of dealing, course of performance or usage of trade and any liability in relation to such matters is expressly excluded.

7.4 The Supplier makes no representations or warranties regarding the Data Protection Product's compliance with Applicable Laws specifically applicable to the Customer or industry and exclude all liability associated therewith.

7.5 The Supplier shall not be liable for any delays, delivery failures, or any other damage resulting from risks inherent in the use of the internet and electronic communications.

7.6 The Customer acknowledges that no password protected system or data storage can be made entirely impenetrable and agree that the Data Protection Product and Backed-Up Data are not guaranteed against all security threats or vulnerabilities.

7.7 No verbal or written information or advice given by the Supplier of Third-Party Supplier or other party will create any additional liabilities or obligations hereunder.

7.8 To the fullest extent permitted by the Applicable Law, in no event shall either Party be liable for incidental, indirect, special, consequential or punitive damages or costs, regardless of the nature of the claim, arising out of the use or inability to use the Data Protection Product, even is advised of the possibility of such damages (whether such damages arise in contract, tort or otherwise arising out of or in connection with the performance of its obligations under this Schedule). In no event shall the Supplier be liable for the procurement of substitute services or products.

7.9 Subject to clause 9 of the General Conditions (except clause 9.4 which is superseded by this paragraph 7.9), the maximum liability of the Supplier, for all claims and damages (whether such damages arise in contract, tort or otherwise arising out of or in connection with the performance of its obligations under this Schedule) shall be limited in aggregate to a sum equal to the Charges paid for the individual Data Protection Product during the calendar year immediately preceding the month in which the event involving that Data Protection Product giving rise to the claim occurred.

7.10 The exclusions and limitations of liability set forth in this paragraph 7 form the essential bases of this Schedule and have been relied upon by both Parties, and absent such exclusions and limitations of liability, the terms of this Schedule and the Charges applicable to the Data Protection Product would be substantially different.

ANNEX 1 - DEFINITIONS

Administrator means one or more persons or entities authorised by the Customer to manage or use the Data Protection Product on behalf of the Customer, including access to and control of Backed-Up Data. The Customer may have multiple Administrators and we expressly rely on the authorisation and instruction of any Administrator until we receive written instructions to the contrary;

API means an application programming interface;

Backed-Up Data means the data and content that the Customer designates for copying, backup and use with the Data Protection Product;

Backed-Up Site means a Third-Party Supplier application or service with which the Data Protection Product interacts, upon Customer's authorisation, to obtain copies of the Backed-Up Data;

"**Confidential Information**" means all operational written or oral information, disclosed by either party to the other that has been identified by the disclosing party as confidential or that by the nature of the circumstances surrounding disclosure ought reasonably to be treated as confidential, but not including Feedback, Aggregate Data, Log Data or Backed-Up Data;

Data Protection Product means the SaaS Protection product provided through the use of Software, web-based Services, or Devices, including all Enhancements to Products, all subject to these Terms of Use;

Device means any hardware-based component of the Data Protection Product offering;

Enhancement means any upgrade, update or modification to the Data Protection Product. All Enhancements will be subject to the terms in this Schedule;

General Conditions means the Suppliers standard terms and conditions as set forth on the Supplier's website at www.chessict.co.uk/legal and which form part of this Agreement;

"**Intellectual Property Rights**" means all intellectual property rights, however arising and in whatever media, whether or not registered, including patents, copyrights, trademarks, service marks, trade names, design rights, database rights, domain names, trade secrets or other proprietary rights and any applications for the protection or registration of such rights and all renewals and extensions thereof throughout the world;

License Fees means the charges associated with use and license of the Data Protection Product;

Online Portal means a web-based application or interface that contains information related to the Data Protection Product, including the ability to manage, support and use the Data Protection Product;

Set Up Charges means the charges in relation to the initial set of the Data Protection Product;

Special Category Data has the meaning given to it in the GDPR;

Specifications means any documentation, user manuals or other materials relating to the Data Protection Products;

Termination Charges means any compensatory charges payable by the Customer to the Supplier on termination of this Agreement in whole or in part in accordance with clause 8.7 of the General Conditions and as set out in the Order, or if not specified, then an amount equal to the 100% of the License Fees for all remaining months of the Minimum Term, together with any waived Set-Up Charges;

User means an individual affiliated with the Customer and who the Customer authorises to use or have use of the Data Protection Product. For purposes of this Schedule, the Customer will be the owner of the Backed-Up Data and the Customer is responsible for the acts and omissions of its Users;

ANNEX 2 -EUROPEAN DATA PROCESSING ADDENDUM

This European Data Processing Addendum ("**DPA**") amends Schedule 3.9 above and the General Conditions only to the extent the Data Protection Product is used to Process Personal Data covered under the GDPR. In the event of a conflict, the terms of this DPA will take precedence.

1. Definitions

Capitalised words are defined in this section or when first used throughout this DPA or the applicable Product Terms of Use.

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, where "control" refers to the power to direct or cause the direction of the subject entity, whether through ownership of voting securities, by contract or otherwise.

"**Controller**", "**Data Subject**", "**Processor**", **Processing**" will have the meaning set forth in Article 4 of the GDPR.

"**Data Subject Request**" means a request made by or on behalf of a Data Subject to exercise a right for access to, rectification, objection, erasure or other applicable right recognized by the GDPR of that Data Subject's Personal Data.

"**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 regard to the Processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC and, from the date the United Kingdom may no longer be a member of the European Union, the corresponding data privacy and protection legislation of the United Kingdom.

"**Personal Data**" means information relating to an identified or identifiable natural person (Data Subject) covered under the GDPR that is directly or indirectly submitted, stored or Processed via use of the Product by Customer, its Affiliates, clients or end users.

"**Subprocessor**" means a third party that, by reason of its role in performing services on behalf of the Third-Party Supplier with respect to its provision of a Product, may have logical access to Personal Data covered by this DPA.

Duration of Processing/Term of DPA

This DPA and the Third-Party Supplier's Processing of Personal Data will terminate automatically upon termination of the Agreement and of any post termination period during which the Third-Party Supplier makes Personal Data available for export by Customer, until its final deletion.

Controller/Processor Roles

For purposes of this DPA, the parties agree that the Third-Party Supplier is a Processor of Personal Data. This DPA does not apply where the Third-Party Supplier is a Controller of Personal Data.

The Customer may act either as a Controller or Processor, as applicable, of Personal Data. If Customer is not the Controller of Personal Data, Customer represents and warrants to the Third Party Supplier that Customer has the right and authority to appoint it as a Processor and provide instructions, and such actions have been authorised by the appropriate Controller of the Personal Data.

The Customer has sole responsibility for the quality, ongoing accuracy, legality and scope of Personal Data and the means by which Customer acquired Personal Data. The Customer represents and warrants that it has sufficient rights and all third party consents as may be necessary and appropriate for the use of the Personal Data with the Data Protection Product and that its submission of Personal Data to will comply with the GDPR and all applicable laws.

Processing of Personal Data

The Third-Party Supplier will Process the Personal Data only on the instructions of Supplier or the Customer, including through the Customer's use and configuration of the features within the Product. The Customer instructs the Third Party Supplier to Process the Customer Personal Data (a) to provide the applicable Data Protection Product and related technical and administrative support consistent with the Agreement and this DPA; (b) as further instructed via Customer's use of the Product; and (c) to comply with other reasonable instructions provided by the Supplier (via email or support tickets) that are consistent with the nature and scope of the Data Protection Product.

Subject Matter and Nature of Processing

The subject matter and scope of Processing is the Third-Party Supplier's provision of the Product, including related technical and administrative support (through management portals or otherwise) in accordance with the terms of the Agreement. The Third-Party Supplier will Process Personal Data that is provided directly or indirectly by Customer, its clients or end users to it for the purpose of providing the Data Protection Product that is the subject of the Agreement.

Data Subject Requests

If Third Party Supplier receives a Data Subject Request related to the Data Protection Product, to the extent it is able to do so, and it is legally permitted, the Third Party Supplier will notify the Supplier and/or direct the Data Subject to make the request directly to Customer.

The Customer is responsible for responding to any Data Subject Requests. Taking into account the nature of the Processing, the Supplier will provide Customer with commercially reasonable assistance in responding to a Data Subject Request, to the extent legally permitted, if such Data Subject Request is reasonably possible consistent with the functionality of the Product and is required under applicable law. To the extent legally permitted, Customer will be responsible for any costs arising from the Supplier's assistance.

Duty of Confidentiality

The Third-Party Supplier ensures that its personnel engaged in the processing Personal Data have committed to maintain the confidentiality of Personal Data by requiring such personnel to execute written confidentiality agreements.

Data Deletion

Within a reasonable amount of time following expiration or termination of the Agreement plus any post termination period during which the Customer has the ability to export Personal Data, the Third-Party Supplier will delete Personal Data. The Customer hereby instructs the Third-Party Supplier to delete all Personal Data after such period. It is Customer's responsibility to export any Personal Data prior to its deletion.

Personal Data Breach

If the Third Party Supplier becomes aware of and confirms a breach of its security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data covered by the GDPR in its custody or control, it will, without undue delay, notify the Supplier and exercise best efforts to mitigate the effects and to minimize any damage resulting from such a security incident.

The Customer agrees that an unsuccessful security incident will not be subject to this section. An unsuccessful security incident includes but is not limited to things such as attempts at unauthorised access to Personal Data or to any of the Third-Party Supplier's equipment or facilities storing Personal Data, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorised access to traffic data that does not result in access beyond IP addresses or headers).

The Third-Party Supplier's obligation to report or respond to a security incident will not be construed as an acknowledgement of any fault or liability of the Third-Party Supplier with respect to the security incident. The Third-Party Supplier will have no obligation to respond to any incidents caused by Customer or anyone acting with Customer's authorisation.

Subprocessing

The Customer acknowledges and agrees that the Third-Party Supplier's Affiliates may be retained as Subprocessors and that it and its Affiliates respectively may engage third party Subprocessors as needed to provide a Product. The Customer hereby consents to the use of Subprocessors as described in this section.

The Customer further acknowledges that the Third-Party Supplier may engage other third party Subprocessers. The Third-Party Supplier maintains a list of its Subprocessers and is required to notify the Supplier of any new Subprocessers. The Supplier can provide the Customer with a list of the Third-Party Supplier's Subprocessers upon request.

Should the Customer object to the use of a Subprocesser it must notify the Suppler promptly in writing, explaining the reasonable grounds for objection. The Supplier will liaise with the Third-Party Supplier to establish if it can make a change to the Customer's configuration or use of the Product to avoid use of the objected Subprocessor. If the Third-Party Supplier is unable to do so within a reasonable period, the Customer shall be permitted to terminate the Agreement or the relevant Data Protection Product.

The Third-Party Supplier is required to use Subprocessors that have executed written contracts containing obligations that are substantially similar to those of under this DPA.

A Product or Product management portal may provide links or integrations or an API which may be used to facilitate integrations to or from third party products or services ("Third Party Applications"). If the Customer elects to integrate with, enable, access or use an API to interact with such Third Party Applications it does so at its own risk and the Third Party Supplier and the Supplier have no responsibility or liability for any Personal Data processed by or through such Third Party Applications. The Customer expressly acknowledges and agrees that all enabled Third Party Applications are expressly authorised by the Customer and the Supplier and the Third Party Supplier are not a co-processor, subprocessor or controller with respect to any Personal Data processed by or on behalf of the Customer through a Third Party Application.

Audit

The Supplier will cooperate with any Customer audit to verify the Supplier's and Third Party Supplier's compliance with its obligations under this DPA by making available, subject to non-disclosure obligations, third party audit reports, where available, descriptions of security controls and other information reasonably requested by Customer regarding security practices and policies.

Taking into account the nature of the Processing and the information available to the Supplier and Third Party Supplier, the Supplier will provide, at Customer's cost if legally allowed, commercially reasonable cooperation and assistance regarding Customer's compliance obligations described in Articles 32-36 of the GDPR.

Limitation of Liability

To the maximum extent allowed by Applicable Law, the total combined liability for the Supplier and the Customer and any of their Affiliates arising out of or related to this DPA is subject to the exclusions and limitations of liability set forth in the Agreement. Any regulatory penalties imposed on either party resulting from this DPA will count toward such liability cap.

Security

The Third-Party Supplier maintains commercially reasonable technical and organisational measures to protect against accidental or unlawful access, destruction, loss or alteration of Personal Data under its control. The Third-Party Supplier may modify such measures, provided that any changes will not result in a material degradation of the security measures.

A Product or Product management portal may make available certain Customer controlled security features, which may include multi-factor authentication, administrative access controls and local encryption. The Third-Party Supplier makes available best practices for Customer to adopt to help protect against accidental or unlawful access, destruction, loss or alteration of Personal Data. The Customer is responsible for securing Personal Data under its control, including but not limited to properly configuring and using available Customer controlled security features.

Transfers of Personal Data

The Third-Party Supplier can allow the Customer the ability to use a data centre located in the European Economic Area ("EEA") or the United Kingdom for Processing of Personal Data. For all such Products, the Customer is responsible for using an appropriate data centre location in the EEA or the UK. Certain data related to technical and administrative support for a Product or its management portal ("Metadata") may be hosted in the U.S. even if Customer uses a data centre located in the EEA or the UK.

The Third Party Supplier self-certify to and comply with the EU-U.S. and Swiss-U.S. Privacy Shield as a transfer mechanism regarding the transfer of Personal Data from the European Union, the EEA, Switzerland and the United Kingdom to the U.S. Transfers of Metadata and Personal Data to the U.S. are validated through the Third-Party Supplier's EU-U.S. and Swiss-U.S. Privacy Shield certification.

The foregoing will not apply if the Third-Party Supplier adopts an alternative GDPR recognized compliance standard for the lawful transfer of Personal Data outside the EEA, Switzerland or the United Kingdom.

The Customer acknowledges and agrees that the Supplier will receive and relay all notices from the Third-Party Supplier related to this DPA, including those notices required by Applicable Law.

It is Customer's responsibility to maintain current, accurate contact information within the applicable administrative portal for the Data Protection Product for purposes of facilitating all notices.

General

The Supplier reserves the right to modify this DPA, including if different GDPR recognised compliance standards become available, or as needed to maintain compliance with the GDPR or other applicable law, or where the Third Party Supplier modifies its terms and conditions with the Supplier.