Prism 339

End User Licence Agreement (“EULA”)

Between

(1) Prism 339 Limited

And

(2) INSERT COMPANY NAME

Dated

This Agreement dated 03 September 2025

BETWEEN

(1) **Prism 339 Limited** ("**PL**") a company incorporated in England and Wales (10339481) having its registered office at 28 Orchard Road, St Annes On Sea, FY8 1PF (the "**Supplier**"); and

(2) **XXXXX** (registration number) whose registered office is at XXXX (the "**Customer**").

each of "**Supplier**" and "**Customer**" being a "**Party**" and collectively the "**Parties**"

BACKGROUND

A. The Customer is contracting with the Supplier on behalf of the insolvency practitioners who have taken the relevant appointment over the relevant entity.

B. The Customer holds bank statements and has authority to allow them to be processed and analysed into a spreadsheet document.

C. The Supplier is a software company and a skilled and experienced provider of data processing services who have developed certain proprietary bank statement analysis software (**Software**) designed for insolvency practitioners.

D. The Customer, having conducted appropriate due diligence and being satisfied that it is appropriate to do so, has selected the Supplier to provide the Services subject to the terms and conditions set out in this Agreement, together with its Schedules.

IT IS AGREED AS FOLLOW:

1. Interpretation

1.1. In this Agreement, unless the context otherwise required, the following words and expressions shall have the following meanings:

"Agreement" or "**EULA"** means this agreement including any Schedules, and any amendments to this Agreement from time to time.

"Charges" means the "**Per Bank Account Analysis fee"**

"Confidential Information" means the Supplier Confidential Information and the Customer Confidential Information.

"Data Protection Laws" means all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR (which has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018); the Data Protection Act 2018 (and regulations made thereunder); and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications); and the guidance and codes of practice issued by the UK Information Commissioner or other relevant regulatory authority and which are applicable to a party.

“Documentation” Knowledge base and how-to guides stored within the Prism339 portal.

“Effective Date” means the date of execution of this Agreement.

“Force Majeure Event” means an event, or a series of related events, that is outside the reasonable control of the Party affected (including failures of the internet or any public telecommunications network, which are not caused by any acts or omission of the Party, hacker attacks, denial of service attacks, virus or other malicious software attacks or infections, power failures, industrial disputes affecting any third Party, changes to the law, disasters, explosions, fires, floods, riots, terrorist attacks and wars).

“Intellectual Property Rights” means all intellectual property rights wherever in the world, whether registrable or unregistrable, registered or unregistered, including any application or right of application for such rights (and these “intellectual property rights” include copyright and related rights, database rights, confidential information, trade secrets, know-how, business names, trade names, trademarks, service marks, passing off rights, unfair competition rights, patents, petty patents, utility models, semi-conductor topography rights and rights in designs).

“Customer Confidential Information” means any information disclosed by the Customer to the Supplier during the Term (whether disclosed in writing, orally or otherwise) that at the time of disclosure was marked or described as “confidential” or should have been understood by the Supplier (acting reasonably) to be confidential.

“Customer Personal Data” means any Personal Data that is processed by the Supplier on behalf of the Customer in relation to this Agreement.

“Supplier Confidential Information” means any information disclosed by the Supplier to the Customer during the Term (whether disclosed in writing, orally or otherwise) that at the time of disclosure was marked or described as “confidential” or should have been reasonably understood by the Customer to be confidential.

“Personal Data” has the meaning given to it in the Data Protection Laws applicable in the United Kingdom from time to time.

“Schedule” means any schedule attached to the main body of this Agreement.

“Services” means any services that the Supplier provides to the Customer, or has an obligation to provide to the Customer, under this Agreement.

“Software Defect” means the specification for the Software set out in Schedule 1 and in the Documentation, as it may be varied by the written agreement of the Parties from time to time.

“Software” means the Software code in human-readable form or any part of the Software code in human-readable form, including code compiled to create the Software or decompiled from the Software, but excluding interpreted code comprised in the Software.

1.2. The Schedules form part of this Agreement and shall have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Schedules.

2. Licence

2.1. The Supplier hereby grants access to the Data Protection Laws compliant portal to the Customer from the date of supply of the Software to the Customer until the end of the Agreement.

2.2. The rights granted to the Customer must not be exercised for any purpose except the Customer's internal business purposes.

2.3. The Customer may not sub-license and must not purport to sub-license any rights granted without the prior written consent of the Supplier.

2.4. The Software may only be used by the officers, agents and employees of the Customer and their clients unless the Supplier gives its consent in writing, such consent not to be unreasonably withheld.

2.5. The Customer must comply with the end user licence agreement (EULA) and must ensure that all persons who use the Software with the authority of the Customer comply with the EULA.

3. Supplier obligations

3.1. Provide training to the Customer staff during the implementation stage and will maintain a dedicated point a contact for all support and system related queries.

3.2. Provide new templates for any statement (including credit cards) provided by a UK bank in a standard tabular structure, within a mutually agreeable timescale.

3.3. Maintain and support the portal including bug fixes or regulated updates, if any.

3.4. Provide a solution able to handle both soft copies of the bank statements (preferably PDF or tiff format) and scanned copies of the statements.

3.5. Supplier agrees to only use the data for the purpose of producing the output report, keep all information confidential, and not pass to any third party except as required by law.

3.6. Supplier undertakes to not transfer data outside of the EU without the prior written consent of the Customer.

3.7. Supplier will maintain a record of all categories of processing activities carried out on behalf of the Customer in accordance with GDPR Article 30(2) (or UK equivalent).

4. Customer Obligations

4.1. Customer confirms that all information submitted has been obtained lawfully, and has the right to share it with Supplier.

4.2. Customer has no responsibility for the legality, reliability, integrity, accuracy and quality of the input file and the Supplier acknowledges that the Customer can only provide the information as is provided to them.

4.3. Customer consents to terms inside data being searched remotely on search engines and other databases.

4.4. Customer consents to images of single digits, unreadable by OCR, being viewed by human eye.

4.5. Customer will provide users of the Service with sufficient technical resources (including any required 3rd party licenses) to utilise both the portal and analysis output.

4.6. Customer will use reasonable endeavours to support the Supplier by following the Supplier's instructions regarding the document download, so full enjoyment of the Service can be sustained.

4.7. Allow the Supplier access to its staff to liaise with them to configure any bespoke business logic for the analysis.

5. Fees and Payments

5.1. The Customer must pay the Charges in accordance with the payment terms specified in Schedule 2.

5.2. All amounts stated in or in relation to this Agreement are, unless the context requires otherwise, exclusive of any applicable value added taxes, which will be added to those amounts and payable by the Customer to the Supplier.

5.3. The Customer must pay the Charges by bank transfer using such payment details as are notified by the Supplier to the Customer.

5.4. If the Customer does not pay any amount properly due to the Supplier under this Agreement, the Supplier may:

a) charge the Customer interest on the overdue amount at the rate of 8% per annum above the Bank of England base rate; or

b) claim interest and statutory compensation from the Customer pursuant to the Late Payment of Commercial Debts (Interest) Act 1998.

6. Confidentiality obligations

6.1. The Supplier must:

a) keep the Customer Confidential Information strictly confidential;

b) not disclose the Customer Confidential Information to any person without the Customer's prior written consent, and then only under conditions of confidentiality approved in writing by the Customer;

c) use the same degree of care to protect the confidentiality of the Customer Confidential Information as the Supplier uses to protect the Supplier's own confidential information of a similar nature, being at least a reasonable degree of care.

6.2. The Customer must:

a) keep the Supplier Confidential Information strictly confidential;

b) not disclose the Supplier Confidential Information to any person without the Supplier's prior written consent, and then only under conditions of confidentiality approved in writing by the Supplier;

c) use the same degree of care to protect the confidentiality of the Supplier Confidential Information as the Customer uses to protect the Customer's own confidential information of a similar nature, being at least a reasonable degree of care.

6.3. No obligations are imposed with respect to a Party's Confidential Information if that Confidential Information:

a) is known to the other Party before disclosure under this Agreement and is not subject to any other obligation of confidentiality;

b) is or becomes publicly known through no act or default of the other Party; or

c) is obtained by the other Party from a third party in circumstances where the other Party has no reason to believe that there has been a breach of an obligation of confidentiality.

6.4. The restrictions in this Clause do not apply to the extent that any Confidential Information is required to be disclosed by any law or regulation, by any judicial or governmental order or request, or pursuant to disclosure requirements relating to the listing of the stock of either Party on any recognised stock exchange.

6.5. The provisions of this Clause shall continue in force following the termination of this Agreement.

7. Data protection

7.1. This agreement and this clause is subject to the Data Processing Agreement at Schedule 4. References to Data Processor in the Data Processing Agreement is in reference to the Supplier and reference to the Data Controller is in reference to the Customer.

7.2. Supplier shall allow for audits of its Data Processing activity by the Customer or the Customer's designated auditor.

7.3. Customer is responsible for ensuring that it complies with all applicable laws relating to privacy and data protection in its use of the Services.

7.4. Supplier is not liable to the Customer for breaches of Personal Data stemming from the Customer's failure to protect such data. Including, but not limited to, inappropriate distribution of reports and emails, disclosure of login credentials.

7.5. Each Party shall comply with the Data Protection Laws with respect to the processing of the Customer Personal Data.

7.6. The Supplier shall promptly inform the Customer if, in the opinion of the Supplier, an instruction of the Customer relating to the processing of the Customer Personal Data infringes the Data Protection Laws.

7.7. Notwithstanding any other provision of this Agreement, the Supplier may process the Customer Personal Data if and to the extent that the Supplier is required to do so by any law or regulation, or by any judicial or governmental order or request. In such a case, the Supplier shall inform the Customer of the legal requirement before processing, unless that law prohibits such information.

7.8. The Supplier shall ensure that persons authorised to process the Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.9. The Supplier and the Customer shall each implement appropriate technical and organisational measures to ensure an appropriate level of security for the Customer Personal Data.

7.10. The Supplier must not engage any third party to process the Customer Personal Data without the prior specific or general written authorisation of the Customer. In the case of a general written authorisation, the Supplier shall inform the Customer at least 14 days in advance of any intended changes concerning the addition or replacement of any third-party processor, and if the Customer objects to any such changes before their implementation, then the Supplier must not implement the changes.

7.11. The Supplier shall, insofar as possible and taking into account the nature of the processing, take appropriate technical and organisational measures to assist the Customer with the fulfilment of the Customer's obligation to respond to requests exercising a data subject's rights under the Data Protection Laws.

7.12. The Supplier shall assist the Customer in ensuring compliance with the obligations relating to the security of processing of personal data, the notification of personal data breaches to the supervisory authority, the communication of personal data breaches to the data subject, data protection impact assessments and prior consultation in relation to high-risk processing under the Data Protection Laws.

7.13. The Supplier must notify the Customer of any Personal Data breach affecting the Customer Personal Data without undue delay and, in any case, not later than 24 hours after the Supplier becomes aware of the breach.

7.14. The Supplier shall, at the request of the Customer, return all data ("**Data"**) to the Customer. This includes but is not limited to;

a) All data stored about the Customer;

b) all Customer Confidential Information;

c) all personal data.

7.15. The Supplier shall, at the request of the Customer immediately delete all data and copies of the data, regardless of the format of the data, including but not limited to;

a) All data stored about the Customer;

b) all Customer Confidential Information;

c) all personal data.

7.16. If any changes or prospective changes to the Data Protection Laws result or will result in one or both Parties not complying with the Data Protection Laws in relation to processing of Personal Data carried out under this Agreement, then the Parties shall use their best endeavours promptly to agree such variations to this Agreement as may be necessary to remedy such non-compliance.

7.17. The Supplier shall not transfer or otherwise process any Customer Personal Data outside the UK or EEA unless the prior written consent of the Customer has been obtained and the following conditions are fulfilled:

a) the Customer or the Supplier has provided appropriate safeguards in relation to the transfer;

b) the data subject has enforceable rights and effective legal remedies;

c) the Supplier complies with its obligations under the Data Protection Laws by providing an adequate level of protection to any Customer Personal Data that is transferred; and

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

8. Warranties

8.1. The Supplier warrants to the Customer that:

a) the Supplier has the legal right and authority to enter into this Agreement and to perform its obligations under this Agreement;

b) the Supplier will comply with all applicable legal and regulatory requirements applying to the exercise of the Supplier's rights and the fulfilment of the Supplier's obligations under this Agreement; and

c) the Supplier has or has access to all necessary know-how, expertise and experience to perform its obligations under this Agreement.

8.2. The Supplier warrants to the Customer that:

a) the Software as provided will conform in all respects with the Software;

b) the Software shall incorporate security features reflecting the requirements of good industry practice.

8.3. The Supplier warrants to the Customer that the Software, when used by the Customer in accordance with this Agreement, will not breach any laws, statutes or regulations applicable under English law.

8.4. The Supplier warrants to the Customer that the Software will not infringe the Intellectual Property Rights of any person in any jurisdiction and under any applicable law and there is no outstanding infringement claim or threat of any claim for infringement of any such Intellectual Property Rights.

8.5. If the Supplier reasonably determines, or any third party alleges, that the use of the Software by the Customer in accordance with this Agreement infringes any person’s Intellectual Property Rights, the Supplier may, acting reasonably at its own cost and expense:

a) modify the Software in such a way that it no longer infringes the relevant Intellectual Property Rights, providing that any such modification must not introduce any Software Defects into the Software and must not result in the Software failing to conform with the Software; or

b) procure for the Customer the right to use the Software in accordance with this Agreement.

8.6. The Customer warrants to the Supplier that it has the legal right and authority to enter into this Agreement and to perform its obligations under this Agreement.

8.7. All of the Parties’ warranties and representations in respect of the subject matter of this Agreement are expressly set out in this Agreement. To the maximum extent permitted by applicable law, no other warranties or representations concerning the subject matter of this Agreement will be implied into this Agreement or any related contract.

8.8. Supplier does not warrant that the Service, the Documentation, or any content, document or feature of the Service will be error-free or uninterrupted, or that any defects or errors or omissions will be corrected.

8.9. The Supplier does not and cannot verify or confirm the accuracy, integrity or completeness of any Transaction Data, Consumer Data or other Data Sources, and does not provide any warranty in this regard. In particular, The Supplier does not warrant that the Data Sources available to The Supplier provide a complete picture of the financial or other relevant data in respect of any report.

8.10. The Documentation and other materials provided by the supplier could include typographical errors or technical inaccuracies.

9. Acknowledgements and warranty limitations

9.1. The Customer acknowledges that the Software is only designed to be compatible with that software specified as compatible in the Software; and the Supplier does not warrant or represent that the Software will be compatible with any other software.

9.2. The Customer acknowledges that the Supplier will not provide any legal, financial, accountancy or taxation advice under this Agreement or in relation to the Software and, except to the extent expressly provided otherwise in this Agreement, the Supplier does not warrant or represent that the Software or the use of the Software by the Customer will not give rise to any legal liability on the part of the Customer or any other person.

10. Indemnities

10.1. The Supplier shall indemnify and shall keep indemnified the Customer against any and all liabilities, damages, losses, costs and expenses (including legal expenses and amounts reasonably paid in settlement of legal claims) suffered or incurred by the Customer and arising directly or indirectly as a result of any breach by the Supplier of this Agreement (a “**Supplier Indemnity Event**”).

10.2. The Customer must:

a) upon becoming aware of an actual or potential Supplier Indemnity Event, notify the Supplier;

b) provide to the Supplier all such assistance as may be reasonably requested by the Supplier in relation to the Supplier Indemnity Event; and

c) not admit liability to any third party in connection with the Supplier Indemnity Event or settle any disputes or proceedings involving a third party and relating to the Supplier Indemnity Event without the prior written consent of the Supplier (such consent not to be unreasonably withheld or delayed).

10.3. The indemnity protection set out in this Clause shall be subject to the limitations and exclusions of liability set out in Clause **Error! Reference source not found.** of this Agreement.

11. Limitations and exclusions of liability

11.1. Nothing in this Agreement will:

a) limit or exclude any liability for death or personal injury resulting from negligence;

b) limit or exclude any liability for fraud or fraudulent misrepresentation;

c) limit any liabilities in any way that is not permitted under applicable law; or

d) exclude any liabilities that may not be excluded under applicable law.

e) limit or exclude Supplier’s liability for any loss incurred by **[INSERT COMPANY]** (and its affiliates and personnel) arising out of third-party claims that software or any other products infringe any Intellectual Property Rights.

11.2. The limitations and exclusions of liability set out in this Clause and elsewhere in this Agreement:

govern all liabilities arising under this Agreement or relating to the subject matter of this Agreement, including liabilities arising in contract, in tort (including negligence) and for breach of statutory duty, except to the extent expressly provided otherwise in this Agreement.

11.3. Neither Party shall be liable to the other Party in respect of any losses arising out of a Force Majeure Event.

11.4. Neither Party shall be liable to the other Party in respect of any loss of profits or anticipated savings.

11.5. Neither Party shall be liable to the other Party in respect of any loss of revenue or income.

11.6. Neither Party shall be liable to the other Party in respect of any loss of use or production.

11.7. Neither Party shall be liable to the other Party in respect of any loss of business, contracts or opportunities.

11.8. Neither Party shall be liable to the other Party in respect of any loss or corruption of any data, database or software.

11.9. Neither Party shall be liable to the other Party in respect of any special, indirect or consequential loss or damage.

11.10. The aggregate liability of each Party to the other Party under this Agreement shall not exceed the total amount paid and payable by the Customer to the Supplier under this Agreement.

12. Force Majeure Event

12.1. If a Force Majeure Event gives rise to a failure or delay in either Party performing any obligation under this Agreement (other than any obligation to make a payment), that obligation will be suspended for the duration of the Force Majeure Event.

12.2. A Party that becomes aware of a Force Majeure Event which gives rise to, or which is likely to give rise to, any failure or delay in that Party performing any obligation under this Agreement, must:

a) promptly notify the other; and

b) inform the other of the period for which it is estimated that such failure or delay will continue.

12.3. A Party whose performance of its obligations under this Agreement is affected by a Force Majeure Event must take reasonable steps to mitigate the effects of the Force Majeure Event.

13. Termination

13.1. Either Party may terminate this Agreement immediately by giving written notice of termination to the other Party if:

a) the other Party commits any material breach of this Agreement, and the breach is not remediable;

b) the other Party commits a material breach of this Agreement, and the breach is remediable but the other Party fails to remedy the breach within the period of 30 days following the giving of a written notice to the other Party requiring the breach to be remedied; or

c) the other Party persistently breaches this Agreement irrespective of whether such breaches collectively constitute a material breach.

13.2. Either Party may terminate this Agreement immediately by giving written notice of termination to the other Party if:

a) the other Party:

(i) is dissolved;

(ii) ceases to conduct all (or substantially all) of its business;

(iii) is or becomes unable to pay its debts as they fall due;

(iv) is or becomes insolvent or is declared insolvent; or

(v) convenes a meeting or makes or proposes to make any arrangement or composition with its creditors;

b) an administrator, administrative receiver, liquidator, receiver, trustee, manager or similar is appointed over any of the assets of the other Party;

c) an order is made for the winding up of the other Party, or the other Party passes a resolution for its winding up (other than for the purpose of a solvent company reorganisation where the resulting entity will assume all the obligations of the other Party under this Agreement); or

d) if that other Party is an individual:

(i) that other Party dies;

(ii) as a result of illness or incapacity, that other Party becomes incapable of managing his or her own affairs; or

(iii) that other Party is the subject of a bankruptcy petition or order.

13.3. For the avoidance of doubt, Clause 13.2 shall only apply to the Customer or the Supplier, and it does not relate to the insolvency proceedings that are being handled by the Customer.

13.4. The Supplier may terminate this Agreement immediately by giving written notice to the Customer if:

a) any amount due to be paid by the Customer to the Supplier under this Agreement is unpaid by the due date and remains unpaid upon the date that that written notice of termination is given; and

b) the Supplier has given to the Customer at least 30 days written notice, following the failure to pay, of its intention to terminate this Agreement.

14. Effects of termination

14.1. Except to the extent that this Agreement expressly provides otherwise, the termination of this Agreement shall not affect the accrued rights of either Party.

14.2. Within 30 days following the termination of this Agreement for any reason:

a) the Customer must pay to the Supplier any Charges in respect of Services provided to the Customer before the termination of this Agreement and in respect of licences in effect before the termination of this Agreement.

14.3. For the avoidance of doubt, access to the Prism Portal shall terminate upon the termination of this Agreement; and, accordingly, the Customer must immediately cease to use the Software upon the termination of this Agreement.

14.4. If the Supplier so requests the Customer shall procure that a director/authorised person of the Customer certifies to the Supplier, in a written document signed by that person and provided to the Supplier within 5 Business Days following the receipt of the

Supplier's request, that the Customer has fully complied with the requirements of this Clause.

15. Notices

15.1. Any notice given under this Agreement must be in writing, whether or not described as "written notice" in this Agreement.

15.2. Any notice given by the Customer to the Supplier under this Agreement must be sent by recorded signed-for post.

15.3. Any notice given by the Supplier to the Customer under this Agreement must be sent by recorded signed-for post.

16. No waivers

16.1. No breach of any provision of this Agreement will be waived except with the express written consent of the Party not in breach.

16.2. No waiver of any breach of any provision of this Agreement shall be construed as a further or continuing waiver of any other breach of that provision or any breach of any other provision of this Agreement.

17. Severability

17.1. If a provision of this Agreement is determined by any court or other competent authority to be unlawful and/or unenforceable, the other provisions will continue in effect.

17.2. If any unlawful and/or unenforceable provision of this Agreement would be lawful or enforceable if part of it were deleted, that part will be deemed to be deleted, and the rest of the provision will continue in effect.

18. Third party rights

18.1. This Agreement is for the benefit of the Parties, and is not intended to benefit or be enforceable by any third party.

18.2. The exercise of the Parties' rights under this Agreement is not subject to the consent of any third party.

19. Variation

19.1. This Agreement may not be varied except by means of a written document signed by or on behalf of each Party.

20. Entire agreement

20.1. The main body of this Agreement and the Schedules shall constitute the entire agreement between the Parties in relation to the subject matter of this Agreement, and shall supersede all previous agreements, arrangements and understandings between the Parties in respect of that subject matter.

20.2. Neither Party will have any remedy in respect of any misrepresentation (whether written or oral) made to it upon which it relied in entering into this Agreement.

21. Law and jurisdiction

21.1. This Agreement shall be governed by and construed in accordance with English law.

21.2. Any disputes relating to this Agreement shall be subject to the exclusive jurisdiction of the courts of England.

22. Interpretation

22.1. In this Agreement, a reference to a statute or statutory provision includes a reference to:

a) that statute or statutory provision as modified, consolidated and/or re-enacted from time to time; and

b) any subordinate legislation made under that statute or statutory provision.

22.2. The Clause headings do not affect the interpretation of this Agreement.

22.3. In this Agreement, general words shall not be given a restrictive interpretation by reason of being preceded or followed by words indicating a particular class of acts, matters or things.

AGREED by the Parties on the date set out at the head of this Agreement.

Signed by)
for and on behalf of) Director
PRISM 339 LIMITED)

Signed by)

for and on behalf of) Partner

XXXX)

SCHEDULE 1

Basic Steps

1. Register on app.prism.com and, once accepted, upload the scan of your choice to us (note that illegible or outsize scans will be rejected under our fair use policy).
2. Complete tick boxes confirming; 1) authority to upload and 2) agreement to commercial terms.
3. Notice of your report available in download portal for a period of 14 days
4. **NOTE:** Once the extracted file has been made available, we will store it for 14 days. If you lose your copy, we do not have a backup file stored on our servers after this time.

SCHEDULE 2

Per Bank Account Analysis fee

- The Customer will pay the Supplier for the Services performed pursuant to this Agreement a sum of **£200.00 plus VAT** where due **("Per Bank Account Analysis fee").**

- **This charge is applied to each bank account and not each case uploaded to the Prism portal.**

Charges Payment Terms

- The Supplier will invoice the Customer on or shortly after the analysis file has been made available to the Customer.

- Every bank account uploaded will receive a separate invoice relating to said account.

- It is expected that the Customer will recover these charges as a Category One Disbursement and the invoice will clearly state the name of the bank account uploaded.

SCHEDULE 3

Service Levels

1. Interpretation

1.1. "Office Hours" means weekdays, excluding bank holidays, between the hours of 9:00am and 5:00pm.

2. Upgrades

2.1. Supplier shall keep the Customer reasonably informed during the Term of its plans for the release of Upgrades; however, except to the extent that the parties agree otherwise in writing, the Supplier shall have no obligation to release Upgrades with features requested by the Customer. However, the Supplier will take into account the opinions of the Customer in relation to plans for the release of Upgrades.

3. Help Desk

3.1. Supplier shall make available to Customer a helpdesk in accordance with the provisions of the Agreement.

3.2. Customer may use this helpdesk for the purposes of requesting and, where applicable, receiving technical support.

3.3. Supplier will ensure the helpdesk is available by telephone, email and by using the Supplier web-based ticketing system.

3.4. Supplier will ensure that the helpdesk is operational and adequately staffed during business hours and during the Term.

3.5. Customer shall ensure that all requests for technical support that it may make from time to time shall be made via the helpdesk.

4. Response and Resolution

4.1. Support requests made by Customer will be prioritised and responded to within a timeframe based on severity.

4.1.1. **CRITICAL** – Representing a complete loss of service or a significant feature that is completely unavailable, and no workaround exists. Response within 2 business hours.

4.1.2. STANDARD – Representing intermittent issues and a reduced quality of service where a workaround may be available. Response within 4 business hours.

4.1.3. GENERAL – Representing product queries, feature requests and general usability questions. Response within 8 business hours.

4.2. Customer accepts that support outside of 'Office Hours' may not always be provided.

5. Limitations and Exclusions

5.1. Supplier is not responsible for supporting any modification or extensions to the Software performed by any party other than Supplier, other than work undertaken under the instruction or guidance of Supplier. However, if required, Supplier will assist in such matters on a chargeable consultancy basis.

SCHEDULE 4

Data Processing Agreement

1. Definitions

1.1 For the purposes of this Schedule, the following expressions bear the following meanings unless the context otherwise requires:

“Affiliate” means, with respect to any entity, any other entity directly or indirectly controlling or controlled by, or under common control with, such entity;

“Applicable Data Protection Laws” means all applicable laws, statutes, declarations, decrees, directives, legislative enactments, orders, ordinances, regulations, rules or other binding instruments in relation to the Processing or protection of Personal Data, to include (but not limited to) the GDPR, UK GDPR, UK Data Protection Act (2018) and e-Privacy Directive (in each case as amended, consolidated, re-enacted or replaced from time to time);

“Data Subject”, “Personal Data”, “Process”, “Processed” or “Processing” shall each have the meaning as set out in the GDPR;

“e-Privacy Directive” means Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector;

“GDPR” means Regulation 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;

“Regulator” means any data protection supervisory authority which has jurisdiction over a Data Controller’s Processing of Personal Data;

“Sub-processor” means any person appointed by or on behalf of the Data Processor (subject to the terms and conditions of this Data Processing Agreement) to process personal data on behalf of the Data Controller in connection with the Agreement;

“Third Country” means, with respect to GDPR, all countries outside the scope of the data protection laws of the European Economic Area, excluding countries approved as providing adequate protection for Personal Data by the European Commission from time to time; and, with respect to the UK GDPR, any country outside the UK, excluding countries approved as providing adequate protection for Personal Data by the UK from time to time; and

“UK GDPR” has the meaning specified in the UK Data Protection Act, as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

2. Data Processor’s Obligations

2.1 To the extent the Data Processor Processes Personal Data on behalf of the Data Controller, it shall:

2.1.1 process the Personal Data only on documented instructions from the Data Controller and to the extent reasonably necessary for the performance of the Agreement, unless required to Process such Personal Data by European Union, EU Member State or UK law; in such a case, the Data Processor shall, unless legally prohibited to do so, inform the Data Controller of that legal requirement before Processing;

2.1.2 ensure that its personnel authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and are aware of their responsibility for the security of the Personal Data that they receive or have access to;

2.1.3 implement and maintain industry-standard or better administrative, technical and physical safeguards with respect to the Personal Data. Without limiting the foregoing, implement appropriate technical and organisational security measures, including, as appropriate, (i) the pseudonymisation of Personal Data, (ii) ensuring the ongoing confidentiality, integrity, availability and resilience of Processing systems and services, (iii) restoring the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, and (iv) regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing and protection against any unauthorised or unlawful Processing of the Personal Data;

2.1.4 taking into account the nature of the Processing, assist the Data Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controller’s obligation to respond to requests for exercising the Data Subject’s rights laid down in the Applicable Data Protection Laws, including requests to amend, correct, transfer, block, or delete Personal Data or the right to object, restrict processing, not to be subject to automated decision making or access and/or receive a copy of their data in a commonly used machine readable format;

2.1.5 promptly carry out a request from Data Controller to amend, correct, transfer, block or delete any of the Personal Data necessary to allow the Data Controller to comply with its responsibilities under Applicable Data Protection Laws;

2.1.6 immediately (and in no event later than 72 hours after discovery) notify the Data Controller in writing upon becoming aware of any improper, unauthorized or unlawful access to, use of, or disclosure of, or any other event which affects the availability, integrity or confidentiality of Personal Data which is Processed by Data Processor under or in connection with the Agreement (“Security Incident”). The Data Processor shall be obliged to provide the Data Controller with all information necessary for the compliance with the Data Controller’s obligations pursuant to Applicable Data Protection Laws and will provide all reasonable cooperation with respect to the investigation of any Security Incident;

2.1.7 assist the Data Controller in ensuring compliance with the obligations to (i) implement appropriate technical and organisational security measures, (ii) notify if required Personal Data breaches to Regulators and/or individuals, and (iii) conduct data protection impact assessments and, if required, prior consultation with Regulators;

2.1.8 at the choice of the Data Controller, delete or return all the Personal Data to the Data Controller after the end of the provision of services relating to Processing, and delete existing copies of the Personal Data unless storage of the Personal Data is required by law;

2.1.9 make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in this Schedule and Applicable Data Protection Laws, and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller to verify that the Data Processor's Processing of the Personal Data is in compliance with this Schedule and Applicable Data Protection Law; and

2.1.10 unless legally prohibited to do so, notify the Data Controller promptly if the Data Processor (or any sub-processor) is required by law, order or regulation to disclose the Personal Data to any person other than the Data Controller.

2.2 The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction of the Data Controller infringes the Applicable Data Protection Laws.

3. Changes in Applicable Data Protection Laws

3.1 The Data Processor shall take all steps reasonably requested by the Data Controller to ensure that the Data Controller's Personal Data is processed in compliance with the GDPR, including (i) any guidance on the interpretation of its provisions once it takes effect, or (ii) if changes to the membership status of a country in the European Union or the European Economic Area require modification, the GDPR and any guidance on the interpretation of its provisions as so modified.

4. International Transfers

4.1 The Data Processor will not Process the Personal Data in, or transfer Personal Data to, a Third Country without the prior written approval of the Data Controller.

4.2 Where the Data Controller approves of the transfer of Personal Data to a Third Country, the Data Processor shall ensure that such processing takes place in accordance with the relevant provisions of GDPR/UK GDPR Articles 44-50.

4.3 Where any such transfer shall rely on standard contractual clauses, the Data Processor shall, upon the Data Controller's request, procure that such Sub-processor enter into the standard contractual clauses directly with the Data Controller.

5. Sub-Processing

5.1 The Data Processor shall not subcontract any of its processing operations performed on behalf of the Data Controller under the Agreement without the prior written consent of the Data

Controller. Where the Data Processor subcontracts its obligations, with the consent of the Data Controller, it shall do so only by way of a written agreement with the Sub-processor which imposes the same obligations on the Sub-processor as are imposed on the Data Processor under this Schedule, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of Applicable Data Protection Laws. The Data Processor will provide a copy of such agreement to the Data Controller on request.

5.2 In the event that the Data Processor engages a Sub-processor for carrying out specific Processing activities on behalf of the Data Controller, where that sub-processor fails to fulfil its obligations, the Data Processor shall remain fully liable under the Applicable Data Protection Laws to the Data Controller for the performance of that Sub-processor's obligations.