DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is effective as of the date of the last signature of Data Technology Limited's terms and conditions ("Effective Date") by and between Data Technology Limited, a company incorporated in England with company number 02154023 and registered address C/O Sterlings Ltd, Lawford House, Albert Place, London, England, N3 1QA ("DT") and the party identified below ("Customer"):
Name: [*]
Address: [*]
Company Number: [*]

The Customer has agreed to the terms and conditions of Service of DT. From time to time, those Services require the processing of personal data by DT.

NOW THE PARTIES AGREE AS FOLLOWS:

In consideration of the rights and obligations set out in this DPA, DT and Customer acknowledge and agree that the processing of personal data in respect of the delivery of the Services by DT and receipt of the Services by the Customer shall be governed by this DPA.

1. DEFINITIONS

Terms bearing capitals in this Data Processing Agreement shall have the same meanings given to them in the Agreement unless set out below.

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Agreement**" means DT's terms and conditions available at https://datatechnology.co.uk/hubfs/TsCsIssue1Rev4.pdf, this Data Processing Agreement and any Order Form.

"**Customer Personal Data**" means any Personal Data which DT Processes on behalf of the Customer in the performance of the Services. It does not include Personal Data for which DT is a Controller.

"**Data Protection Legislation**" means all laws and regulations relating to privacy and security of personal data, including but not limited to Regulation (EU) 2016/679 ("GDPR"), the GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018 ("UK GDPR"), the UK Data Protection Act 2018, in each case as amended, replaced or superseded, and any subsequent applicable regulations applicable to personal data processing in accordance with the terms of this Agreement.

"**EEA**" means, for the purpose of this DPA, the European Economic Area (including the European Union) and Switzerland.

"**Personal Data**" means information relating to an identified or identifiable natural person that is governed as individually identifiable information under Data Protection Legislation.

"**Personnel"** means a Party's employees or other workers under their direct control.

"**Security Breach**" means any unauthorised or unlawful destruction, loss, alteration or access to, or disclosure of, Customer Personal Data that is in DT's possession or under DT's control.

"**Termination Date**" means the termination or expiration of the Services under the Agreement between the Parties.

"**Third Country**" means a country where the data protection laws and regulations are not considered to offer an adequate level of protection by (i) the European Commission in respect of Customer Personal Data subject to the GDPR and (ii) by the UK Government in respect of Customer Personal Data subject to the UK GDPR.

"**2021 SCCs**" means the 2021 SCCs Module Two and or Module Three as applicable published under EU Commission Decision 2021/914/EU for EU Personal Data transfers outside the EU to third countries not deemed by the EU Commission to have an adequate level of privacy protection.

"**Controller**", "**Data Subject**", "**Processor**", "**Process/Processed/Processing**", **"Subprocessor**", "**Supervisory Authority**" and **"Third Country"** will be interpreted in accordance with Data Protection Legislation.

2. PROCESSING BY DT OF CUSTOMER PERSONAL DATA

2.1 Details of Processing are as set out in Schedule 1 of this DPA.

2.2 **Purpose of Processing Customer Personal Data.** The Parties agree that the Customer is the Controller and DT is the Processor in relation to the Customer Personal Data that DT processes on the Customer's behalf in the course of providing the Services. For the avoidance of doubt, this DPA does not apply to Personal Data for which DT is a Controller. DT will Process the Customer Personal Data only as set out in the Agreement and perform the Services for the Customer.

2.3 **Disclosure of Customer Personal Data.** Unless otherwise provided for in the Agreement, DT will not disclose to any third party any Customer Personal Data, except, in each case, as necessary to maintain or provide the Services, or, notwithstanding Section 4.5 below, in order to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order).

2.4 **Obligations of DT Personnel.** DT Will ensure that any employees of DT required to access the Customer Personal Data are subject to a binding duty of confidentiality in respect of such Customer Personal Data and take reasonable steps to ensure the reliability and competence of such employees.

2.5 **Instructions.** Customer authorizes and instructs DT to Process Customer Personal Data for the performance of the Services. The Customer shall ensure that its Processing instructions comply with applicable Data Protection Legislations in relation to Customer

Personal Data and that the Processing of Customer Personal Data in accordance with the Customer's instructions will not cause DT to be in breach of any relevant law. The Customer warrants that it has the right and authority under applicable Data Protection Legislation to disclose, or have disclosed, Customer Personal Data to DT to be Processed by DT for the Services and that the Customer has obtained all necessary consents and provided all necessary notifications required by Data Protection Legislation with respect to the Processing of Customer Personal Data by DT. The Customer will not disclose Customer Personal Data to DT, or instruct DT to Process Customer Personal Data, for any purpose not permitted by applicable law, including Data Protection Law. DT will notify the Customer if DT becomes aware that, and in DT's reasonable opinion, an instruction for the Processing of Customer Personal Data given by the Customer violates Data Protection Legislation, it being acknowledged that DT is not under any obligation to undertake additional work, screening or legal assessment to determine whether Customer's instructions are compliant with Data Protection Legislation.

2.6 **Assistance to the Customer.** Upon a written request, DT will provide reasonable cooperation and assistance necessary to assist the Customer, and at the Customer's cost, insofar as required by Data Protection Legislation and as it relates to Processing by DT for the Services, in fulfilling the Customer's obligations to respond to requests from Data Subjects exercising their rights (notwithstanding the Customer's obligations in Section 6) and/or to carry out data protection impact assessments. (ii) notify a personal data breach to the relevant supervisory authority; (iii) communicate a personal data breach to the affected data subject(s); (iv) carry out data protection impact assessments; and/or (v) submit to prior consultation with the relevant supervisory authority.

2.7 **Compliance with Data Protection Legislations.** Each Party will comply with all Data Protection Legislations applicable to it in relation to performance of this DPA for the purposes of the Agreement.

3. SECURITY

3.1 **Security of Data Processing.** DT will implement and maintain appropriate technical and organizational measures to protect Customer Personal Data against unauthorised or unlawful Processing and against accidental or unlawful loss, destruction, alteration or damage, and against unauthorized disclosure or access. These measures will be appropriate to the harm, which might result from any unauthorized or unlawful Processing, accidental loss, destruction, damage or theft of the Customer Personal Data taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, of the Customer Personal Data which is to be protected. At a minimum, these will include the measures set out in the Appendix to this DPA.

3.2 **Notification of a Security Breach.** Upon becoming aware of a Security Breach, DT will notify the Customer without undue delay and take reasonable steps to identify the effects of the Security Breach. A notification by DT to the Customer of a Security Breach under this DPA is not and will not be construed as an acknowledgement by DT of any fault or liability of DT with respect to the Security Breach.

3.3 **Notification Mechanism.** Security Breach notifications, if any, will be delivered to Customer by any means DT selects, including via email. It is the Customer's responsibility to ensure that it provides DT with accurate contact information and secure transmission at all times.

4. SUBPROCESSORS

4.1 **Authorized Subprocessors.** The Customer agrees that DT may use its Affiliates and other Subprocessors to fulfil its contractual obligations under this DPA or to provide certain Services on its behalf as set out in the Order Form and notified to the Customer from time to time.

4.2 **Subprocessor Obligations.** Where DT uses a Subprocessor as set forth in this Section 4, DT will:
(i) enter into a written agreement with the Subprocessor and will impose on the Subprocessor contractual obligations no less protective than the overall obligations that DT has provided under this DPA; and (ii) restrict the Subprocessor's access to and use of Customer Personal Data only to provide the Services. For the avoidance of doubt, where a Subprocessor fails to fulfil its obligations under any Sub-Processing agreement or any applicable Data Protection Legislation with respect to Customer Personal Data, DT will remain liable, subject to the terms of this DPA, to the Customer for the fulfilment of DT's obligations under this DPA.

4.3 **Appointing a New Subprocessor.** At least thirty (30) days before DT engages any new Subprocessor to carry out Processing activities on Customer Personal Data, DT will provide notice of such update to the Subprocessor list through the applicable website. If the Customer is entitled to do so under applicable Data Protection Legislation and as it relates to the Processing of Customer Personal Data by the Subprocessor, the Customer may make reasonable objections in writing to DT and marked for the attention of the Data Protection Officer within the 30-day period regarding the appointment of the new Subprocessor. After receiving such written objection DT will either: (i) work with the Customer to address the Customer's objections to its reasonable satisfaction, (ii) instruct the Subprocessor not to Process Customer Personal Data, provided that the Customer accepts that this may impair the Services (for which DT shall bear no responsibility or liability), or (iii) notify the Customer of an option to terminate this DPA and the applicable order form for Services which cannot be provided by DT without the use of the objected-to new Subprocessor. If DT does not receive an objection from the Customer within the 30-day objection period, the Customer will be deemed to have consented to the appointment of the new Subprocessor.

5. THIRD COUNTRY DATA TRANSFERS

5.1 **Transfers of Customer Personal Data.** Where Customer Personal Data subject to the GDPR and/or the UK GDPR is transferred by DT to a Subprocessor located in a Third Country, DT will ensure that such transfer is compliant with applicable Data Protection Legislation. For transfers from DT to its affiliate in India, DT has 2021 SCCs in place with that affiliate. Where the 2021 SCCs are replaced by obligations under any successor or alternate Third Country lawful transfer mechanism, DT will enter into such successor or alternative transfer mechanism with its Subprocessors.

6. CUSTOMER PERSONAL DATA REQUESTS

6.1 **Government Surveillance of Customer Personal Data. DT** agrees that it will not provide access to Customer Personal Data of an EEA/UK Customer transferred under this DPA to any government or intelligence agency, except where its legal counsel has determined it is strictly relevant and necessary to comply with the law or a valid and binding order of a government authority (such as pursuant to a court order). If a law enforcement agency or other government authority provides DT with a demand for access to such Customer Personal Data, DT will attempt to redirect the law enforcement agency to request the Customer Personal Data directly from the Customer. If compelled by law to provide access to such Customer Personal Data to a law enforcement agency or other government authority, and only after a determination of such is made by legal counsel, then DT will, unless DT is legally prohibited from doing so: (1) give Customer notice of the demand no later than five (5) days after such demand is received to allow Customer to seek recourse or other appropriate remedy to adequately protect the privacy of EEA/UK Data Subjects, and DT shall provide reasonable cooperation in connection with the Customer seeking such recourse; and (2) in any event, provide access only to such Customer Personal Data as is strictly required by the relevant law or binding order (having used reasonable efforts to minimize and limit the scope of any such access).

7. AUDITS

7.1 **Audit Requests.** Without prejudice to its other obligations in this DPA, DT will give to the Customer on written request (where such requests shall occur no more than once every 12 months) reasonable information necessary to determine DT's compliance with this DPA and will discuss in good faith any audits reasonably required by the Customer, conducted by a third party agreed to by the Parties. Such audits, if agreed, must be carried out at the Customer's cost, be conducted in a manner undisruptive to the business of DT and its Affiliates, be conducted subject to the terms of an applicable non-disclosure agreement, and not prejudice other confidential information (including Personal Data of DT, its Affiliates or its other customers.

8. ACCESS AND DELETION OF CUSTOMER PERSONAL DATA

8.1 **Access and Deletion on Termination of the Agreement.** Upon completion of the Services, DT shall, at the option of the Customer, return or delete all Customer Personal Data including copies of back-ups, unless prohibited by law, or the order of a governmental or regulatory body. The Customer shall confirm such return or deletion in writing to DT.

9. MISCELLANEOUS

9.1 **Governing Law and Jurisdiction.** This DPA, and any dispute or claim arising out of or in connection with the same or its subject matter or formation (including non-contractual disputes or claims), shall be governed by the same governing law and jurisdiction as the Agreement.
9.2 **Conflict**. In the event of a conflict between this DPA and the Agreement, this DPA shall prevail.
9.3 **Counterparts and Electronic Signature.** This DPA may be signed in one or more counterparts, and each counterpart will be considered an original agreement, but will not be effective until each Party has executed at least one counterpart. All of the counterparts will together be considered one document. Each Party may sign and deliver this DPA by email or other appropriate electronic signature mechanism, which will be binding.

Agreed to as of the DPA Effective Date by each party's authorized representative:	
Data Technology Ltd: Signature: Name and Title: Company: Date:	Customer: Signature: Name and Title: Company: Date:

APPENDIX
TECHNICAL AND ORGANISATIONAL MEASURES

DT shall undertake appropriate technical and organisational measures for the availability and security of Customer Personal Data and to protect it against unauthorised or unlawful Processing and against accidental or unlawful loss, destruction, alteration or damage, and against unauthorized disclosure or access. These measures, listed below, shall take into account the nature, scope, context and purposes of the Processing, available technology as well as the costs of implementing the specific measures and shall ensure a level of security appropriate to the harm that might result from a Security Breach. While DT may alter its measures in line with evolving security practices and risks, and with due regard to the nature of the Processing, DT will not materially decrease the overall protections of the Customer Personal Data below the aggregate standard of the measures in this Appendix.

1. **Access Controls to Premises and Facilities.** DT maintains technical and organizational measures to control access to premises and facilities, particularly to check authorization, utilizing various physical security controls such as ID cards, keys, alarm systems, surveillance systems, entry/exit logging and door locking to restrict physical access to office facilities.

2. **Access Controls to Systems and Data.** DT operates technical and organizational measures for user identification and authentication, such as logs, policies, assigning distinct usernames for each employee and utilizing password complexity requirements for access to on-premises and cloud- based platforms. In addition, user access is established on a role basis and requires user management, system or HR approval, depending on use. Second-layer authentication may be employed where relevant by way of multi-factor authentication. User access for sensitive platforms is subject to periodic review and testing. DT's IT control environment is based upon industry-accepted concepts, such as multiple layers of preventive and detective controls, working in concert to provide for the overall protection of DT's computing environment and data assets. To strengthen access control, a centralized identity and access management solution is used to manage application access. DT uses on-boarding and off-boarding processes to regulate access by DT Personnel.

3. **Disclosure Controls.** DT maintains technical and organizational measures to transport, transmit and communicate or store data on data media (manual or electronic). For certain data transfers, bearing in mind the risk and sensitivity of the data, DT may employ encrypted network or similar transfer technologies. Personnel must utilize a dedicated or local VPN network to access internal resources and/or industry-standard authentication and secure communication mechanisms to access cloud- based systems. Logging and reporting are utilized for validation and review purposes. Third party Subprocessors are subject to privacy and security risk assessments and contractual commitments.

4. **Input Controls.** DT maintains measures in its general IT systems for checking whether relevant data has been entered, changed or removed (deleted), and by whom, such as by way of application-level data entry and validation capabilities. and reporting is utilized for validation and review purposes.

5. **Job Controls.** DT uses technical (e.g., access controls) and organizational (e.g., policies) measures to delineate, control and protect data for which DT is the Controller or the Processor. DT records and delineates the data types for which it is a Controller or a Processor in its record of processing activities under Article 30 (2) GDPR.

6. **Separation Controls.** DT uses segregation standards and protocols between production, testing and development environments of sensitive platforms. Additionally, segregation of data is further supported through user access role segregation.

7. **Availability Controls.** DT maintains measures to assure data availability such as local and/or cloud-based back-up mechanisms involving scheduled and monitored backup routines, and local disaster recovery procedures. DT may supplement these with additional security protections for its business, for example malware protection. Additionally, data centers of a critical nature are required to submit to periodic 3rd party evaluation of operating effectiveness for significant controls ensuring data availability. Relevant systems and data center locations are protected through the use of industry-standard firewall capabilities.

8. **Other Security Controls.** DT maintains (i) regular control evaluation and testing by audit (internal and/or external), on an as-needed basis, (ii) individual appointment of system administrators, (iii) user access by enterprise IDP, (iv) binding policies and procedures for DT's Personnel, and (v) regular security and privacy training. Policies will clearly inform Personnel of their obligations (including confidentiality and associated statutory obligations) and the associated consequences of any violation.

SCHEDULE 1

PERSONAL DATA PROCESSING – DESCRIPTION OF PROCESSING

Subject matter of the Processing	To provide the Services in accordance with the terms of the Agreement.
Nature and Purpose of Processing	
Data Processing activities	Use for the purpose of providing the Services.
Categories of Data Subjects	Customer's users (past, current and future employees)
Types of Personal Data	Users: Name, contact details, role, login details and IP address.
Special Category or Sensitive Personal Data	None
Duration of Processing	In accordance with this DPA
Sub-Processors	Business Intelligence & Integration Solutions Pvt Ltd, Hiranandani Zenia, Hiranandani Circle, Central Avenue, Hiranandani Estate Thane West, 400607, Maharashtra, India.
Location of Processing	UK and India