DATA PROCESSING TERMS

1. DEFINITIONS AND INTERPRETATION

The following definitions and rules of interpretation apply in these Data Processing Terms together with all other definitions contained in the accompanying Order Form, SaaS Agreement and Service Level Agreement.

Appropriate Technical and Organisational Measures: has the meaning given to such term in Data Protection Legislation (including, as appropriate, the measures referred to in Article 32(1) of the GDPR).

Customer Data: the Customer Data (NPD) and the Customer Data (PD) provided by the Customer or any User to the Supplier or accessed by the Supplier on the Customer System in the course of providing the Services, and any other Personal Data Processed by the Supplier (as Data Controller) on behalf of the Customer.

Customer Data (NPD): all non-Personal Data supplied by the Customer to the Supplier from time to time other than the Customer Data (PD) during the Term.

Customer Data (PD): the Personal Data supplied by the Customer to the Supplier from time to
time during the Term.

Customer System: any information technology system or systems owned or operated by the
Customer from which Customer Data is received (or accessed) by the Supplier in accordance with this Agreement.

Data: any data or information, in whatever form, including but not limited to images, still and moving, and sound recordings.

Data Controller: has the meaning given to such term in Data Protection Legislation.

Data Processor: has the meaning given to such term in Data Protection Legislation.

Data Protection Legislation: means the Data Protection Acts 1988 -2018 and Directive 95/46/EC, any other applicable law or regulation relating to the processing of personal data and to privacy (including the E-Privacy Directive and the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 ("**E-Privacy Regulations**"), as such legislation shall be amended, revised or replaced from time to time, including by operation of the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") (and laws implementing or supplementing the GDPR, and laws amending or supplementing the E- Privacy Regulations).

Data Protection Officer: a data protection officer appointed pursuant to Data Protection Legislation.

Data Subject: an individual who is the subject of Personal Data (including any User).

Delete: to remove or obliterate Personal Data such that it cannot be recovered or reconstructed.
EEA: European Economic Area.

Intellectual Property Rights: patents, utility models, rights to inventions, copyright and neighbouring and related rights, trademarks and service marks, business names and domain
names, rights in get-up and trade dress, goodwill and the right to sue for passing off or unfair competition, rights in designs, database rights, rights to use, and protect the confidentiality of,
confidential information (including know-how and trade secrets), and all other intellectual property rights, in each case whether registered or unregistered and including all applications and rights to apply for and be granted, renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world.

ODPC: Office of the Data Protection Commissioner.

Personal Data: has the meaning set out in Data Protection Legislation and relates only to personal data, or any part of such personal data, in respect of which the Customer is the Data Controller, and in respect of which the Supplier is the Data Processor under this Agreement.

Personal Data Breach: means any “personal data breach" as defined in the GDPR in respect of the Personal Data caused by the Supplier.

Processing: has the meaning given to such term in Data Protection Legislation and Processed and Process shall be interpreted accordingly.

Representatives: a Party's employees, officers, representatives, advisers or subcontractors involved in the provision or receipt of the Services.

Restricted Transfer: any transfer of Personal Data to countries outside of the EEA which are not subject to an adequacy decision by the European Commission, where such transfer would be prohibited by Data Protection Legislation.

Security Features: any security feature, including any encryption, pseudonymisation, key, PIN,
password, token or smartcard.

Standard Contractual Clauses: the contractual clauses dealing with the transfer of Personal Data outside the EEA, which have been approved by (i) the European Commission under Data
Protection Legislation, or (ii) by the ODPC or an equivalent competent authority under Data Protection Legislation.

Sub-processor: has the meaning given to such term in Clause under heading Sub Processors.

Supplier System: any information technology system or systems owned or operated by the Supplier to which Customer Data is delivered or on which the Services are performed in accordance with this Agreement.

Term: the term of the Agreement.

Users: end users of the Customer's app/website/products/services.

1.1 A reference to a statute or statutory provision is a reference to it as amended, extended or re-enacted from time to time.

1.2 A reference to a statute or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.

1.3 References to Clauses and Appendices in this Schedule are to the Clauses and Appendices of this Schedule.

1.3 In the event that (i) either Party is required to enter into the Standard Contractual Clauses in accordance with Clause under heading Restricted Transfers of this Schedule, and (ii) there is any conflict or ambiguity between any provision contained in this Schedule and any provision contained in such Standard Contractual Clauses, the Standard Contractual Clauses shall take precedence.

2. SUPPLIER'S OBLIGATIONS

2.1 The Supplier shall:

2.1.1 only make copies of the Customer Data to the extent reasonably necessary for the Business Purpose (which, for clarity, includes back-up, mirroring (and similar availability enhancement techniques), security, disaster recovery and testing of the Customer Data);

2.1.2 not extract, reverse-engineer, re-utilise, use, exploit, redistribute, re-disseminate, copy or store the Customer Data other than for the Business Purpose; and

2.1.3 not do anything that may materially damage the reputation of the Customer.

2.2 The Supplier shall notify the Customer in writing without delay of any situation or envisaged development that shall in any way influence, change or limit the ability of the Supplier to Process the Customer Data (PD) as set out in this Agreement.

2.3 The Supplier shall promptly comply with any request from the Customer requiring the Supplier to amend, transfer or Delete any of the Customer Data.

2.4 At the Customer's request, the Supplier shall provide to the Customer a copy of all Customer Data held by the Supplier in the format and on the media reasonably specified by the Customer.

2.5 At the Customer's request, the Supplier shall provide to the Customer such information and such assistance as the Customer may reasonably require, and within the timescales reasonably specified by the Customer, to allow the Customer to comply with its obligations under Data Protection Legislation, including but not limited to assisting the Customer to:

4.5.1 comply with its own security obligations with respect to the Personal Data;

4.5.2 discharge its obligations to respond to requests for exercising Data Subjects' rights with respect to the Personal Data;

4.5.3 comply with its obligations to inform Data Subjects about serious Personal Data Breaches;

4.5.4 carry out data protection impact assessments and audit data protection impact assessment compliance with respect to the Personal Data; and

4.5.5 the consultation with the ODPC following a data protection impact assessment, where a data protection impact assessment indicates that the Processing of the Personal Data would result in a high risk to Data Subjects.

2.6 Any proposal by the Supplier to in any way use or make available the Customer Data other than as provided for pursuant to this Agreement shall be subject to prior written approval of the Customer.

3. SUPPLIER'S EMPLOYEES

3.1 The Supplier shall ensure that access to the Customer Data is limited to those employees who need access to the Customer Data strictly to meet the Supplier's obligations under this Agreement and/or to comply with Data Protection Legislation; and in the case of any access by any employee, such part or parts of the Customer Data as is strictly necessary for performance of that employee's duties.

3.2 The Supplier shall ensure that all employees that have access to the Customer Data:

5.2.1 are informed of the confidential nature of the Customer Data and are subject to an appropriate statutory obligation of confidentiality or have committed themselves to a binding duty of confidentiality in respect of such Customer Data;

5.2.2 have undertaken training in the laws relating to handling Personal Data; and

5.2.3 are aware both of the Supplier's duties and their personal duties and obligations under Data Protection Legislation and this Agreement.

3.3 The Supplier shall take reasonable steps to ensure the reliability of any of the Supplier's
employees (or approved agents/contractors) who have access to the Customer Data.

5.6 RECORDS

6.1.1 The Supplier shall keep at its normal place of business detailed, accurate and up-to-date records (including in electronic form) relating to all categories of Processing activities carried out on behalf of the Customer containing;

6.2 details of the purposes of such processing;

6.2.1 a general description of the security measures taken in respect of the Personal Data, including details of any Security Features and the Appropriate Technical and Organisational Measures;

6.2.2 the name and contact details of the Supplier; any sub-processor; where applicable, the Supplier's representatives; and where applicable any Data Protection Officer appointed by the Supplier;

6.2.3 the categories of Data Subjects and categories of Personal Data Processed by the Supplier on behalf of the Customer;

6.2.4 the time limits for erasure of the Personal Data; and

6.2.5 details of any non-EEA Personal Data transfers, and the safeguards in place in respect of such transfers.

7. AUDITS

7.1 The Customer shall have the right to examine and review the use by the Supplier of the Customer Data provided to the Supplier by the Customer for the purposes of ascertaining that such Customer Data has been used and Processed in accordance with the terms of this Agreement.

7.2 The Supplier shall grant to the Customer (or representatives of the Customer) on reasonable advance notice a right of access to the Supplier's premises during Normal Business Hours for the purposes of such examination and review, and the Supplier shall give all necessary assistance to the conduct of such examinations/audits during the Term. The requirement to give reasonable advance notice will not apply if the Customer believes that the Supplier is in breach of any of its obligations under this Agreement.

7.3 The examination and review by the Customer of the use by the Supplier of the Personal Data may include, but shall not be limited to, a review of the existing internal compliance regime of the Supplier in relation to:

7.3.1 business processes and nature of interactions with customers;

7.3.2 existing audit procedures on business activities and financial reporting, and the governance of such procedures;

7.3.3 staff vetting, hiring and training procedures;

7.3.4 data access requests and the purpose/duration for which Personal Data is Processed/kept;

7.3.5 reporting of data breaches; and

7.3.6 the named director or senior person (or Data Protection Officer (if applicable to the Supplier)) within the organisation with responsibility for audit and business process rigour.

7.4 After each audit, the Customer may (but shall not be obliged to) provide a report to the Supplier detailing the extent of compliance with the provisions of this Agreement. The Supplier shall respond as required to the findings and recommendations of any Customer audit report and shall provide information requested by the Customer on the implementation by the Supplier of any required actions.

7.5 In the event that the audit process determines that the Supplier is non-compliant with the provisions of this Agreement, the Customer may, by notice in writing, deny further access to the
Customer Data and the termination provisions in the Agreement may be, by notice in writing, invoked.

7.6 Without prejudice to the Customer's right of audit under this Clause, to the extent permitted under Data Protection Legislation, the Supplier may demonstrate its and, if applicable its Sub- processors', compliance with its obligations under this Agreement through its compliance with a certification scheme or code of conduct approved under Data Protection Legislation.

8. CONFIDENTIALITY

8.1 The Supplier acknowledges that the Customer's Confidential Information includes any Customer Data.

8.2 The term Confidential Information does not include any information that[9]:

8.2.1 is or becomes generally available to the public (other than as a result of its disclosure by the receiving Party or its Representatives in breach of this Clause 8);

8.2.2 was available to the receiving Party on a non-confidential basis before disclosure by the disclosing Party;

8.2.3 was, is, or becomes, available to the receiving Party on a non-confidential basis from a person who, to the receiving Party's knowledge, is not bound by a confidentiality agreement with the disclosing Party or otherwise prohibited from disclosing the information to the receiving Party;

8.2.4 the Parties agree in writing is not confidential or may be disclosed; or

8.2.5 is developed by or for the receiving Party independently of the information disclosed by the disclosing Party.

8.3 Each Party shall keep the other Party's Confidential Information confidential and shall not:

8.3.1 use any Confidential Information of the other Party except for the Business Purpose; or

8.3.2 disclose any Confidential Information of the other Party in whole or in part to any third party, except as expressly permitted by this Clause 8.

8.4 A Party may disclose the other party's Confidential Information to those of its Representatives who need to know that Confidential Information for the Business Purpose, provided that:

8.4.1 it informs those Representatives of the confidential nature of the Confidential Information before disclosure; and

8.4.2 at all times, it is responsible for the Representatives' compliance with the confidentiality
obligations set out in this Clause 8.

8.5 A Party may disclose Confidential Information to the extent required by law, by any governmental or other regulatory authority, or by a court or other authority of competent jurisdiction provided that, as far as it is legally permitted to do so, it gives the other Party as much notice of the disclosure as possible.

8.6 Each Party reserves all rights in its Confidential Information. No rights or obligations in respect of a Party's Confidential Information, other than those expressly stated in this Agreement, are granted to the other Party, or are to be implied from this Agreement.

8.7 The provisions of this Clause 9 shall continue to apply after termination of this Agreement.

9. DATA SUBJECT REQUESTS

9.1 The Supplier shall co-operate with and assist the Customer, including but not limited to employing Appropriate Technical and Organisational Measures, in respect of the fulfilment of the Customer's obligations to respond to requests from a Data Subject exercising his/her rights under Data Protection Legislation.

9.2 The Supplier shall notify the Customer within twenty four (24) hours if it receives:

9.2.1 a request from a Data Subject for access to that person's Personal Data;

9.2.2 any communication from a Data Subject seeking to exercise rights conferred on the Data Subject by Data Protection Legislation in respect of the Personal Data; or

9.2.3 any complaint or any claim for compensation arising from or relating to the Processing of the Personal Data.

9.3 The Supplier shall not disclose the Personal Data to any Data Subject or to a third party other than at the request of the Customer or as provided for in this Agreement, or as required by law, in which case the Supplier shall to the extent permitted by law inform the Customer of that legal requirement before the Supplier discloses the Personal Data to any Data Subject or third party.

9.4 The Supplier shall not respond to any request from a Data Subject except on the documented instructions of the Customer or Authorised Person or as required by law, in which case the Supplier shall to the extent permitted by law inform the Customer of that legal requirement before the Supplier responds to the request.

10. DATA PROTECTION OFFICER

10.1 The Supplier shall appoint a Data Protection Officer, if required to do so pursuant to Data Protection Legislation, and provide the Customer with the contact details of such Data Protection Officer.

11. SECURITY

11.2 The Supplier shall, in accordance with its requirements under Data Protection Legislation, implement Appropriate Technical and Organisational Measures and Security Features to safeguard the Customer Data (PD) from unauthorised or unlawful Processing or

accidental loss, alteration, disclosure, destruction or damage, and that, having regard to the state of technological development and the cost of implementing any measures (and the nature, scope, context and purposes of Processing, as well as the risk to Data Subjects), such measures shall ensure a level of security appropriate to the harm that might result from unauthorised or unlawful Processing

11.3 or accidental loss, alteration, disclosure, destruction or damage and to the nature of the Personal Data to be protected.

11.4 The Supplier shall ensure that the Customer Data provided by the Customer can only be accessed by persons and systems that are authorised by the Supplier and necessary to meet the Business Purpose, and that all equipment used by the Supplier for the Processing of Customer Data shall be maintained by the Supplier in a physically secure environment.

11.5 The Supplier shall make a back-up copy of the Customer Data every week and record the copy on media from which the Customer Data can be reloaded in the event of any corruption or loss of the Customer Data.

12. BREACH REPORTING

12.3 The Supplier shall promptly inform the Customer if any Customer Data is copied, modified, lost or destroyed or becomes damaged, corrupted, or unusable, or if there is any accidental,
unauthorised or unlawful disclosure of or access to the Customer Data. In such case, the Supplier
will restore such Customer Data at its own expense, and will comply will all of its obligations under Data Protection Legislation in this regard.

12.4 The Supplier must inform the Customer of any Personal Data Breaches, or any complaint, notice or communication in relation to a Personal Data Breach, without undue delay, provide sufficient information and assist the Customer in ensuring compliance with its obligations in relation to notification of Personal Data Breaches (including the obligation to notify Personal Data Breaches to the ODPC within seventy two (72) hours), and communication of Personal Data Breaches to Data Subjects where the breach is likely to result in a risk to the rights of such Data Subjects. The Supplier shall co-operate with the Customer and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

12.5 In the event of a Personal Data Breach or any data breach involving the Services, the Supplier shall not make any announcement to the media in respect of such breach without first consulting with the Customer.

13. RESTRICTED TRANSFERS

14.1 A Restricted Transfer may not be made by the Supplier without the prior written consent of the Customer, and if such consent has been obtained, such Restricted Transfer may only be made where there are Appropriate Technical and Organisational Measures in place with regard to the rights of Data Subjects (including but not limited to the Standard Contractual Clauses, Privacy Shield, binding corporate rules, or any other model clauses or transfer mechanism approved by the ODPC).

14.2 Subject to Clause 14.3, in the event of any Restricted Transfer by the Supplier to a contracted Sub-processor, to any affiliate of the Customer or otherwise ("Data Importer") for which consent has been obtained, the Parties shall procure that (i) the Customer (where the Restricted Transfer is being made at the request of the Customer) or the Supplier acting as agent for and on behalf of the Customer (where the Restricted Transfer is being made at the request of the Supplier), and (ii) the Data Importer, shall enter into the Standard Contractual Clauses in respect of such Restricted Transfer.

14.3 Clauses 14.1 or 14.2 shall not apply to a Restricted Transfer if other compliance steps (which may include, but shall not be limited to, obtaining explicit consents from Data Subjects) have been taken to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Legislation.

14. WARRANTIES

16.1 The Supplier warrants, represents and undertakes to the Customer that:

16.1.1 the Supplier will Process the Customer Data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments (including Data Protection Legislation);

16.1.2 the Supplier will maintain Appropriate Technical and Organisational Measures against the unauthorised or unlawful Processing of Customer Data (PD) and against the accidental loss or destruction of, or damage to, Customer Data (PD); and

16.1.3 the Supplier will discharge its obligations under this Agreement with all due skill, care and diligence.

16.2 The Customer does not warrant that the Customer Data:

16.2.1 is or are accurate, complete, reliable, secure, useful, fit for purpose or timely;

16.2.2 has or have been tested for use by the Supplier or any third party; or

16.2.3 will be suitable for or be capable of being used by the Supplier or any third party.