MAXIMIZER SOFTWARE LIMITED – DATA PROCESSING TERMS

These are the data processing terms (**Terms**) of Maximizer Software Limited, a company registered in England and Wales (company number 01896712) whose registered office is at 2-4 Packhorse Road, Gerards Cross, SL9 7QE (**Maximizer**) which are incorporated in and form part of any subscription agreement (cloud or on-premise) (**Agreement**) which Maximizer enters into with any customer (**Customer**) for Maximizer CRM.

1. DEFINITIONS

1.1 In these Terms the follow definitions apply:

A**pplicable Laws**: means:

(a) To the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom.

(b) To the extent EU GDPR applies, the law of the European Union or any member state of the European Union to which Maximizer is subject.

Applicable Data Protection Laws: means:

(a) To the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of personal data.

(b) To the extent the EU GDPR applies, the law of the European Union or any member state of the European Union to which Maximizer is subject, which relates to the protection of personal data.

Customer Personal Data: any personal data which Maximizer processes in connection with the Agreement, in the capacity of a processor on behalf of the Customer.

EU GDPR: the General Data Protection Regulation (*(EU) 2016/679*).

Maximizer Personal Data: any personal data which Maximizer processes in connection with the Agreement, in the capacity of a controller, for example the business contact details of the Customer's personnel, representatives and agents.

Purpose: the purposes for which the Customer Personal Data is processed, as set out in clause 2.8(a).

UK GDPR: has the meaning given to it in the Data Protection Act 2018.

2. DATA PROTECTION

2.1 For the purposes of this clause 2, the terms **controller**, **processor**, **data subject**, **personal data**, **personal data breach** and **processing** shall have the meaning given to them in the UK GDPR.

2.2 Both parties will comply with all applicable requirements of Applicable Data Protection Laws. This clause 1 is in addition to, and does not relieve, remove or replace, a party's obligations or rights under Applicable Data Protection Laws.

2.3 The parties have determined that, for the purposes of Applicable Data Protection Laws:

(a) Maximizer shall act as controller of any Maximizer Personal Data; and

(b) Maximizer shall process the personal data set out in the Schedule, as a processor on behalf of the Customer.

2.4 Should the determination in clause 2.3 change, then each party shall work together in good faith to make any changes which are necessary to this clause 2 or the Schedule.

- By entering into the Agreement, the Customer consents to (and shall procure all required consents, from its personnel, representatives and agents, in respect of) all actions taken by Maximizer in connection with the processing any Maximizer Personal Data, provided these are in compliance with the then-current version of Maximizer's privacy policy available at **https://www.maximizer.com/about-us/privacy-policy/** (**Privacy Policy**). In the event of any inconsistency or conflict between the terms of the Privacy Policy and these Terms, the Privacy Policy will take precedence.

2.5 Without prejudice to the generality of clause 2.2, the Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of Maximizer Personal Data and Customer Personal Data to Maximizer and the lawful processing of the same by Maximizer for the duration and purposes of the Agreement.

2.6 In relation to the Customer Personal Data, the Schedule sets out the scope, nature and purpose of processing by Maximizer, the duration of the processing and the types of personal data and categories of data subject.

2.7 Without prejudice to the generality of clause 2.2 Maximizer shall, in relation to Customer Personal Data:

(a) process that Customer Personal Data only on the documented instructions of the Customer, which shall be to process the Customer Personal Data for the purposes set out in the Schedule, unless Maximizer is required by Applicable Laws to otherwise process that Customer Personal Data. Where Maximizer is relying on Applicable Laws as the basis for processing Customer Processor Data, Maximizer shall notify the Customer of this before performing the processing required by the Applicable Laws unless those Applicable Laws prohibit the Provider from so notifying the Customer on important grounds of public interest. Maximizer shall inform the Customer if, in the opinion of Maximizer, the instructions of the Customer infringe Applicable Data Protection Legislation;

(b) implement the technical and organisational measures set out in Appendix A of this document to protect against unauthorised or unlawful processing of Customer Personal Data and against accidental loss or destruction of, or damage to, Customer Personal Data, which the Customer has reviewed and confirms are appropriate to

the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures;

(c) ensure that any personnel engaged and authorised by Maximizer to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory or common law obligation of confidentiality;

(d) assist the Customer insofar as this is possible (taking into account the nature of the processing and the information available to Maximizer), and at the Customer's cost and written request, in responding to any request from a data subject and in ensuring the Customer's compliance with its obligations under Applicable Data Protection Laws with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

(e) notify the Customer without undue delay on becoming aware of a personal data breach involving the Customer Personal Data;

(f) at the written direction of the Customer, delete or return Customer Personal Data and copies thereof to the Customer on termination of the Agreement unless Maximizer is required by Applicable Law to continue to process that Customer Personal Data. For the purposes of this clause 2.8(f) Customer Personal Data shall be considered deleted where it is put beyond further use by Maximizer; and

(g) maintain records to demonstrate its compliance with this clause 2.

2.8 The Customer hereby provides its prior, general authorisation for Maximizer to:

(a) appoint processors to process the Customer Personal Data, provided that Maximizer:

(i) shall ensure that the terms on which it appoints such processors comply with Applicable Data Protection Laws, and are consistent with the obligations imposed on Maximizer in this clause 1;

(ii) shall remain responsible for the acts and omission of any such processor as if they were the acts and omissions of Maximizer; and

(iii) shall inform the Customer of any intended changes concerning the addition or replacement of the processors, thereby giving the Customer the opportunity to object to such changes provided that if the Customer objects to the changes and cannot demonstrate, to Maximizer's reasonable satisfaction, that the objection is due to an actual or likely breach of Applicable Data Protection Law, the Customer shall indemnify Maximizer for any losses, damages, costs (including legal fees) and expenses suffered by Maximizer in accommodating the objection.

(b) transfer Customer Personal Data outside of the UK as required for the Purpose, provided that Maximizer shall ensure that all such transfers are effected in accordance with Applicable Data Protection Laws. For these purposes, the Customer

shall promptly comply with any reasonable request of Maximizer, including any request to enter into standard data protection clauses adopted by the EU Commission from time to time (where the EU GDPR applies to the transfer) or adopted by the Commissioner from time to time (where the UK GDPR applies to the transfer).

2.9 Either party may, at any time on not less than 30 days' notice, revise this clause 2 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when replaced by attachment to this agreement).

2.10 Maximizer's total aggregate liability in contract, tort (including negligence and breach of statutory duty howsoever arising), misrepresentation (whether innocent or negligent), restitution or otherwise, arising in connection with the performance or contemplated performance of the Agreement insofar as it relates to the obligations set out in these Terms, or Applicable Data Protection Laws shall be limited to in accordance with the limitation of liability provisions set out in the Agreement.

SCHEDULE

PARTICULARS OF THE PROCESSING

Scope of processing	In providing the Service to a Customer pursuant to the terms of the Agreement, Maximizer shall process Personal Data only to the extent necessary to provide the Service in accordance with the terms of the Agreement, this DPA and the Customer's instructions documented in the Agreement, as updated from time to time. The Customer and Maximizer shall take steps to ensure that any natural person acting under the authority of the Customer or Maximizer who has access to Personal Data does not process them except on the instructions from the Customer unless he or she is required to do so by any Data Protection Law.
Nature of processing	Maximizer will process personal data as necessary to provide the Services under the Agreement for the cloud-based or on-premise Maximizer CRM Live technology. Maximizer does not sell Customer's personal data or Customer end users' personal data and does not share such end users' information with third parties for compensation.
Duration of the processing	Maximizer only processes Personal Data for as long as necessary to meet our contractual and legal obligations or where we have a legitimate business reason for keeping it. We review Personal Data on a case-by-case basis and document the period of retention for each. For further information on how long Personal Data is likely to be kept before being removed from our systems and databases, please contact us directly.
Types of Personal Data	Personal data may include, among other information, personal contact information such as name, address, telephone or mobile number, fax number, email address, and passwords; employment details including employer name, job title and function, employment history, salary and other benefits, job performance and other capabilities, information about education and

	qualifications, identification numbers and business contact details; financial details; goods and services provided; unique IDs collected from mobile devices, network carriers or data providers, IP addresses, behaviour and interest data, and any other data the Customer may elect to include as part of the processing.
Categories of Data Subject	Data subjects may include the Customer's representatives and end users, such as employees, job applicants, contractors, collaborators, partners, customers and users of the Customer and any other data subjects which the Customer may elect to include as part of the processing. Data subjects may also include individuals attempting to communicate or transfer personal data to users of the Maximizer CRM Live technology.

Appendix A

Maximizer CRM Live Cloud Services Technical and Organizational Security Measures

Site Access Control

Personal Data is processed and stored in professionally hosted data centres, which are protected with effective physical access control, including electronic locks, burglar alarms and CCTV monitoring. Only nominated, authorized persons have physical access to data centre facilities.

System Access Control

Each user of data processing systems is authenticated with a personal user account. Shared or group accounts are not used for personal access. Each user account must be approved by a management sponsor, and each user is personally responsible for the user account and the ways in which it is used. User accounts are reviewed and audited regularly, and unnecessary users are removed.

Data Access Control

Access rights to data processing systems are granted to pre-defined roles according to least privilege principle. Access to Personal Data must be justified with a clear and indisputable business need and approved by a management sponsor. Special administrative privileges are granted to an absolute minimum number of users. Access rights are reviewed regularly, and unnecessary rights are removed.

Transfer Control

Electronic transfers of Personal Data in public networks are encrypted. Transfers within a data centre environment may not be encrypted; however, access to networks and processing systems is strictly limited by site and system access control. It is forbidden to store Personal Data to removable media. Backups of Personal Data are encrypted.

Disclosure Control

Data flows of Personal Data are tracked to ensure comprehensive access control and to minimize the risk of accidental or unauthorized data disclosure. New connections and data transfers must be approved by a management sponsor. Transfer of Personal Data to non-production environments, such as testing, is forbidden without explicit customer approval and sufficient data masking.

Input Control

Access to Personal Data is monitored, and an audit trail is created for all data processing systems.. Access logs are considered Personal Data and are protected accordingly. Access logs are stored for a minimum of one (1) year, or for the minimum duration mandated by external compliance requirements.

Order Control

The scope of Personal Data protection and how to deal with customer's instructions is further described in the Personal Data Processing Appendix.

Availability Control

Personal Data is backed up at regular intervals. Copies of data backups are transferred securely to an offsite location for disaster recovery. Data processing systems and infrastructure utilize redundant technologies, and single points of failure are minimized. Recovery time and point objectives are determined, and every effort is made to adhere to them.

Separation Control

Personal Data is processed in dedicated systems that are not shared with other services, unless requested to do so by the client, as part of an integration or extension of the product, applications or corporate entities. Within individual systems and databases, data is segregated with logical access control. Personal Data will not be used for different purposes other than what it has been collected for without explicit customer approval.

Notification Control

Customers will receive a prompt notification in the event of a Personal Data breach, a significant security incident in data processing system, or a material deviation from any of the controls above. In case Personal Data is lost or compromised, customer will be invited to participate in incident resolution, and granted access to applicable logs.