ERP Maestro Standard Data Processing Addendum

I. TERMS AND DEFINITIONS

Terms below shall have the following meanings:

1. "Agreement" means the Software license agreement signed between ERP Maestro, Inc. and the Client.
2. The Company, providing you services through this web application is (referred to hereinafter as ERP Maestro, Inc.), a company duly organized under the law of Florida, having its working address at "6400 N Andrews Ave., Suite 210, Fort Lauderdale, Florida 33309".
3. "ERP Maestro, Inc. Products" means the Software and other products of ERP Maestro, Inc. together with any products that are hereafter designed, developed or marketed by ERP Maestro, Inc.
4. "Client Data" means data submitted, stored, sent or received via the Software by Clients or End Users.
5. "Client Personal Data" means personal data contained within the Client Data.
6. "Data Incident" means a breach of ERP Maestro, Inc. security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Client Data on systems managed by or otherwise controlled by ERP Maestro, Inc. Data Incidents will not include unsuccessful attempts or activities that do not compromise the security of Client Data, Including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
7. "Data Processing Addendum" or "DPA" means this Addendum, which is an inseparable part of the Software license agreement signed between ERP Maestro, Inc. and the Client.
8. "End User" means Person who ultimately uses or is intended to ultimately use the software.
9. "European Data Protection Legislation" means, as applicable, the GDPR, as well as any other applicable EU legislation.
10. "GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the

processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

11. "License" means the Software license granted to the Client by ERP Maestro, Inc. pursuant to the Agreement.
12. “Party” means either ERP Maestro, Inc. or the Client.
13. “Parties” means both ERP Maestro, Inc. and the Client.
14. “Term” means the term set forth in the Agreement.
15. “SaaS model” means a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted by ERP Maestro, Inc. The Software is accessed by Clients via a web browser and/or web-based APIs.
16. “Services” means the services, provided by ERP Maestro, Inc. as described in the Agreement and the Terms of Use for the ERP Maestro, Inc. Services, an inseparable part of the Agreement.
17. “Software” means computer software (Access Analyzer), developed by ERP Maestro, Inc.
18. “Standard Contract Clauses” means the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR.
19. “Subprocessors” means third parties authorized under this Data Processing Addendum to have logical access to and process Client Data in order to provide parts of the Services and related technical support.
20. “Third parties” means any other persons, organizations and authorities, besides ERP Maestro, Inc. and the Client.
21. “Web-site” means the web-based site www.erpmaestro.com as well as web-based application (em.erpmaestro.com or similar URL)

All terms, which have not been explicitly defined above, such as “personal data”, “data subject”, “processing”, “controller”, “processor”, “supervisory authority”, etc. have the meanings given in the GDPR.

II. SCOPE OF ADDENDUM

1. **Software License Agreement**
   a. ERP Maestro, Inc. provides a SaaS (Software as a Service) web-based application which by functionality performs SOD risk analysis and remediation for SAP user authorization. The application supports accounts management with role-based

permissions, creation of tasks, processing business rule books and SAP authorization data, report functionality, Emergency Access Management, Access Review management and a set RESTful API interfaces for partner integration.

b. Parties have signed an Agreement for the use of ERP Maestro, Inc. Software by the Client for the Client's own internal business purposes.

c. Under the Software license agreement ERP Maestro, Inc. agreed to provide the Client with the Services as specified in the Agreement and the Terms of Use.

d. In rendering the Services, the ERP Maestro, Inc. may from time to time be provided with, or have access to, information of the Client which may qualify as personal data within the meaning of the GDPR and other applicable European data protection laws and provisions.

2. GDPR

a. This Data Processing Addendum reflects the Parties' agreement with respect to the terms governing the processing and security of Client Data under the Agreement according to the requirements of GDPR and any other European Data Protection Legislation.

b. The parties acknowledge and agree that the European Data Protection Legislation, Including the GDPR will apply to the processing of Client Personal Data if, the Client Personal Data is personal data relating to data subjects who are in the EU/EEA and the processing relates to the offering to them of goods or services in the EU/EEA or the monitoring of their behavior in the EU/EEA as well as when the processing is carried out in the context of the activities of an establishment of Client in the territory of the EU/EEA.

c. The Parties agree that the sets of data processing and transfers covered by this DPA qualify as commissioned data processing as per Art. 28 of the GDPR with ERP Maestro, Inc. qualifying as processor within the meaning of the GDPR and that they would like to use this DPA as the required contractual processing agreement.

d. In order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Client to ERP Maestro, Inc. of the personal data, the Parties have entered into this DPA.

e. The Parties agree that ERP Maestro, Inc. shall have the right to ask for changes to any part of this DPA to the extent required to satisfy any interpretations, guidance or orders issued by competent Union or Member State authorities, national

implementation provisions, or other legal developments concerning the GDPR requirements for the commissioning of data processors in general or other requirements for the commissioning of data processors. The Parties will agree on the necessary changes in good faith effort taking their obligation to carry out this contractual relationship in compliance with applicable data protection law into account.

3. Processor and Controller

a. ERP Maestro, Inc. is a processor of Client Personal Data.

b. Client is a controller of Client Personal Data.

c. Each Party will comply with the obligations applicable to it under the European Data Protection Legislation with respect to the processing of that Client Personal Data.

d. Client warrants to ERP Maestro, Inc. that Client's instructions and actions with respect to that Client Personal Data, are legitimate and permitted under the applicable European Data Protection Legislation.

e. Client is responsible that the processing activities relating to the personal data, as specified in this DPA, are lawful, fair and transparent in relation to the data subjects concerned.

4. Scope of Processing

a. By entering into this Data Processing Addendum, the Client instructs ERP Maestro, Inc. to process Client Personal Data only in accordance with applicable law: (a) to provide the Services and related technical support; (b) as further specified via Client's use of the Services and related technical support; (c) as documented in the applicable Agreement, Including the applicable Terms of Use and this Data Processing Addendum; and (d) as further documented in any other written instructions given by Client and acknowledged by ERP Maestro, Inc. as constituting instructions for purposes of this Data Processing Addendum.

b. Any further instructions of processing, given by the Client to ERP Maestro, Inc. that go beyond the instructions contained in this DPA or the Agreement shall be considered within the subject matter of the Services Agreement and this DPA and ERP Maestro, Inc. acts of processing shall be considered lawful and compliant with the GDPR and other applicable legislation. It shall be the Clients responsibility to guarantee the legality of any personal data processing of which the Client has given instructions to ERP Maestro, Inc. to perform.

c. The Client acknowledges that the Services, provided by ERP Maestro, Inc. to the Client include, among others described above, the provision by ERP Maestro, Inc. to the Client and all End Users, using the Software on behalf of the Client, of notifications on the scope of Services, their update, upgrade, amendment, new releases, development and/or termination via Newsletters, emails and other electronic and nonelectronic means of communication, which may be applicable.

d. ERP Maestro, Inc. will comply with the instructions described above (Client's Instructions) (including with regard to data transfers) unless EU law requires other processing of Client Personal Data by ERP Maestro, Inc., in which case ERP Maestro, Inc. will inform Client (unless that law prohibits ERP Maestro, Inc. from doing so on important grounds of public interest). Upon providing such notification, ERP Maestro, Inc. is not obliged to follow the Client's instruction.

e. For clarity, ERP Maestro, Inc. will not process Client Personal Data for Advertising purposes or serve Advertising in the Services. Notifications from ERP Maestro, Inc. to the Client and all End Users on the scope of Services, their update, upgrade, amendment, new releases, developments and/or termination via Newsletters, emails and other electronic and nonelectronic means of communication, which may be applicable, shall not be considered advertising, marketing or other activity, not included in the Services. Such notifications shall be considered part of the Services provided by ERP Maestro, Inc. to Client.

f. If at any time the Client or any End User would like to unsubscribe from receiving future emails, he or she must follow the instructions on how to unsubscribe at the bottom of ERP Maestro, Inc. emails.

5. Subject Matter

a. ERP Maestro, Inc. 's provision of the Services and related technical support to Client.

6. Data Subjects

a. The personal data processed concern the following categories of data subjects:
   i. staff of the Client – End Users;
   ii. other subjects, whose personal data is entered by the End Users.

7. Nature and Purpose of the Processing

a. ERP Maestro, Inc. will process Client Personal Data submitted, stored, sent or received by Client, its Affiliates or End Users via the Software for the purposes of providing the Services and related technical support to Client in accordance with the Data Processing Addendum.

8. Duration of the Processing

a. The applicable Term plus the period from expiry of such Term until deletion of all Client Data by ERP Maestro, Inc. in accordance with the Data Processing Addendum, unless the GDPR requires otherwise.

9. Categories of Data and Purpose of its Processing

a. Personal data submitted, stored, sent or received by Client or End Users via the Services may include the following categories of data:

   i. Name and User name– necessary for identification of the Data Subject. The main feature of the Software is to analyze, report on and manage SOD and other types of risk analysis, so it is vital to be able to recognize the person, provisioned and/or performing the respective activities.

   ii. Email address – necessary for authenticating the End Users before allowing its access to the Software and Client Data, Including Client Personal Data, as well as for providing technical support.

   iii. Phone number - necessary for providing technical support and communicating conditions in respect of the Service providing.

   iv. Other data - uploaded by Client and End Users – entering and upload of any other personal data is at the full discretion of the Client.

b. ERP Maestro, Inc. shall not use any other personal data, entered by Client or End User, except for categories of data, described in Section (a) above.

c. It is not ERP Maestro, Inc.'s obligation to monitor personal data, entered or uploaded by Client or End User, to categorize or process it in any other way.

d. It is the Client's responsibility to provide and guarantee that the processing personal data activities, performed by Client and End Users with the Software shall be compliant with the requirements of the GDPR.

10. Method of collection

a. Each User of the Software provides personally the Personal data, entered or uploaded in the Software.

b. Client and End users shall enter third party personal data only with due authorization or in a GDPR compliant manner. Client and End users are responsible for entering somebody else's personal data without acquiring their preliminary due authorization or GDPR complaint consent. ERP Maestro, Inc. does not control the content, entered by Client and End User. ERP Maestro, Inc. has no contact with any third parties, whose personal data

the Client or End User may enter in the software. In the event of a third-party claim or sanctions by a competent authority in respect of entering third party personal data in the Software in violation of GDPR by Client or End User, Client shall compensate ERP Maestro, Inc. for all sustained damages, Including any compensations, administrative penalties and sanctions, reasonable lawyer fees, expenses, etc.

11. Data Subjects

a. Personal data submitted, stored, sent or received via the Services may concern the following categories of data subjects: End Users including Client's employees and contractors; the personnel of Client's Clients, suppliers and subcontractors; and any other person who transmits data via the Services, including individuals collaborating and communicating with End Users.

b. Client shall grant access to End Users after acquainting them to the information, provided to Client in this DPA, the rights of the End Users under the GDPR and the methods of their implementation. Client acknowledges that such provision of information is required by GDPR and is necessary for the implementation of GDPR principals of data protection. Client shall also grant access to End Users, who have accepted the terms and conditions of data protection, Included in this DPA. In the event of a Data Subject claim or sanctions by a competent authority in respect of entering or processing personal data in the Software in violation of GDPR by Client or End User, Client shall compensate ERP Maestro, Inc. for all sustained damages, Including any compensations, administrative penalties and sanctions, reasonable lawyer fees, expenses, etc.

12. Cookies

a. To the extent as permitted under applicable European Data Protection legislation, parties agree that ERP Maestro, Inc. may use Cookies on the Website and collect information about the preferences and interests of the visitors and to analyze data about the people browsing the Website.

b. Information about the collected information and processing of any Website uses cookies shall be used by ERP Maestro, Inc. to improve the quality of the services offered.

c. Disabling Website cookies may affect some features of the Website and these may not work properly or as intended.

13. Additional Services

a. If ERP Maestro, Inc. at its option makes any Additional Services available to Client in accordance with the Terms of Use and if Client opts to install or use those Additional Services, the Services may allow those Additional Services to access Client Personal Data as required for the operation of the Additional Services. For clarity, this Data Processing Addendum shall apply to the processing of personal data in connection with the provision of any Additional Services installed or used by Client, including personal data transmitted out of the EU.

b. Even if the Client has not objected initially to the transfer of data out of EU, the Client may at all times inform in writing ERP Maestro, Inc. that Client does not want personal data to be transferred any more to third parties in case of Additional service integration and ERP Maestro, Inc. shall not transfer in the future such data after the date on which ERP Maestro, Inc. has received the communication from the Client. However, if the Client has initially accepted such transfer and has not later on informed ERP Maestro, Inc. in writing about any objection, it shall be considered that the Client has instructed ERP Maestro, Inc. to provide the Additional Service and execute data transfers until the date of the objection. If the Client objects to such transfer, the Client and the end Users shall not be able to use those Additional Services anymore.

14. Data Deletion

a. ERP Maestro, Inc. will enable Client and/or End Users to delete Client Data during the applicable Term in a manner consistent with the functionality of the Services, if such deletion is in accordance with applicable law. ERP Maestro, Inc. will comply with this instruction as soon as reasonably practicable and within a maximum period of 30 days, unless EU or United States law requires storage.

b. With this DPA the Client instructs ERP Maestro, Inc. to delete on expiry of the applicable Term Client all Client Data (including existing copies) from ERP Maestro, Inc.'s systems in accordance with applicable law. ERP Maestro, Inc. will comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days, unless EU or United States law requires storage. Client acknowledges and agrees that Client will be responsible for exporting, before the applicable Term expires, any Client Data it wishes to retain afterwards.

c. To the extent any Client Data covered by the deletion instruction described in Section (b) is also processed, when the applicable Term expires, in relation to an Agreement with a continuing Term, such deletion instruction will only take effect with respect to such Client Data when the continuing Term expires.

d. For clarity, this Data Processing Addendum will continue to apply to Client Data until its deletion by ERP Maestro, Inc.

15. Data Security

a. ERP Maestro, Inc. will implement and maintain technical and organizational measures to protect Client Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. The Technical and organizational measures include measures to help ensure ongoing confidentiality, integrity, availability and resilience of ERP Maestro, Inc.'s systems and services; to help restore timely access to personal data following an incident; and for regular testing of effectiveness. ERP Maestro, Inc. may update or modify the Technical and organizational Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

b. ERP Maestro, Inc. will take appropriate steps to ensure compliance with the Technical and organizational Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance, Including ensuring that all persons authorized to process Client Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c. Client agrees that ERP Maestro, Inc. will (taking into account the nature of the processing of Client Personal Data and the information available to ERP Maestro, Inc. .) assist Client in ensuring compliance with any of Client's obligations in respect of security of personal data and personal data breaches, Including if applicable Client's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by: (a) implementing and maintaining the Technical and organizational Measures in accordance with the GDPR; (b) complying with the procedures for Data Incidents notification and regulation as required by the GDPR; (c) providing Client with the necessary information and documentation as required by the GDPR.

16. Data Incidents

a. If ERP Maestro, Inc. becomes aware of a Data Incident and if it is required by the GDPR, ERP Maestro, Inc. will notify Client of the Data Incident promptly and without undue delay; and promptly take reasonable steps to minimize harm and secure Client Data.

b. Notifications made pursuant to this section will implement the requirements of the GDPR and will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps ERP Maestro, Inc. recommends Client take to address the Data Incident.

c. Notification of any Data Incident will be delivered to the Email Address of the Client, recorded in the Agreement or, at ERP Maestro, Inc.'s discretion, by direct communication (for example, by phone call or an in-person meeting). Client is solely responsible for ensuring that the Client's Email Address is current and valid.

d. ERP Maestro, Inc. will not assess the contents of Client Data in order to identify information subject to any specific legal requirements. Client is solely responsible for complying with incident notification laws applicable to Client and fulfilling any third-party notification obligations related to any Data Incident.

e. ERP Maestro, Inc.'s notification of or response to a Data Incident under this Section will not be construed as an acknowledgement by ERP Maestro, Inc. of any fault or liability with respect to the Data Incident.

f. Client acknowledges that although ERP Maestro, Inc. will take all reasonable precautions to keep personal data safe and secure, ERP Maestro, Inc. shall not be liable for extraneous circumstances such as theft, communication errors or malicious tampering.

17. Client's Security Responsibilities

a. Client agrees that Client is solely responsible for its use of the Services and the compliance of Client's and End Users' activities with GDPR, Including:

   i. making appropriate use of the Services and the Software to ensure a level of security appropriate to the risk in respect of the Client Data;

   ii. securing the account authentication credentials, systems and devices Client uses to access the Services; and

iii. backing up its Client Data;

b. Client agrees that ERP Maestro, Inc. has no obligation to protect Client Data that Client elects to store or transfer outside of ERP Maestro, Inc.'s and its Subprocessors' systems (for example, offline or on-premise storage), or to protect Client Data by implementing or maintaining Technical and organizational Measures except to the extent Client has opted to use them.

c. Client is solely responsible for reviewing ERP Maestro, Inc.'s Technical and Organizational Measures and evaluating for itself whether the Services, the Technical and organizational Measures and ERP Maestro, Inc.'s commitments under DPA will meet Client's needs, Including with respect to any security obligations of Client under the European Data Protection Legislation, as applicable.

d. Client acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Client Personal Data as well as the risks to individuals) the Technical and organizational implemented and maintained by ERP Maestro, Inc. as set out in this DPA provide a level of security appropriate to the risk in respect of the Client Data.

18. Impact Assessments

a. Client agrees that ERP Maestro, Inc. may (taking into account the nature of the processing and the information available to ERP Maestro, Inc.) assist Client in ensuring compliance with any obligations of Client in respect of data protection impact assessments and prior consultation, Including if applicable Client's obligations pursuant to Articles 35 and 36 of the GDPR, by providing the Client with ERP Maestro, Inc.'s Technical and Organizational Measures and providing other information contained in the applicable Agreement including this Data Processing Addendum.

b. ERP Maestro, Inc. may charge a fee (based on ERP Maestro, Inc.'s reasonable costs) for any assistance under Section (a) above. ERP Maestro, Inc. will provide the Client with details of any applicable fee, and the basis of its calculation, in advance of any such assistance.

c. ERP Maestro, Inc. may object in writing to providing any assistance under Section (a) above at its own discretion, if it will harm or may harm in any way

ERP Maestro, Inc. 's legal rights, business interests, normal course of activities or may be otherwise manifestly unsuitable.

19. Monitoring

a. In order to assist the Client with its legal obligation to diligently choose a service provider, ERP Maestro, Inc. shall monitor, by appropriate means, its own compliance and the compliance of its employees and Sub-processors with the respective data protection obligations of a Processor laid down in Art. 28 of the GDPR and in this DPA in connection with the Services. ERP Maestro, Inc. shall make available to the Client any information necessary to demonstrate compliance with such obligations when required by the GDPR.

20. Reviews and Audits of Compliance

a. ERP Maestro, Inc. has made available for review by Client ERP Maestro, Inc.'s Technical and organizational measures and Standard Contract Clauses with Subprocessors. The Client is responsible to confirm before processing is carried out that ERP Maestro, Inc.'s technical and organizational measures are appropriate and sufficient to protect the rights of the data subjects.

b. If the European Data Protection Legislation requires, ERP Maestro, Inc. will allow Client or an independent auditor appointed by Client to conduct audits to verify ERP Maestro, Inc.'s compliance with its obligations under this Data Processing Addendum. ERP Maestro, Inc. will contribute to such audits by providing information and documentation as described in Section (a) above or to the extend, required by GDPR and Bulgarian data protection legislation.

c. Following receipt by ERP Maestro, Inc. of a request for an audit, ERP Maestro, Inc. and Client will discuss and agree in advance on reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit.

d. ERP Maestro, Inc. may charge a fee (based on ERP Maestro, Inc.'s reasonable costs) for any audit. ERP Maestro, Inc. will provide Client with further details of any applicable fee, and the basis of its calculation, in advance of any such review or audit. Client will be responsible for any fees charged by any auditor appointed by Client to execute any such audit.

e. ERP Maestro, Inc. may object in writing to an auditor appointed by Client to conduct any audit, if the auditor is, in ERP Maestro, Inc.'s reasonable opinion, not suitably qualified or independent, a competitor of ERP Maestro, Inc., or otherwise manifestly unsuitable. Any such objection by ERP Maestro, Inc. will require Client to appoint another auditor or conduct the audit itself.

21. Data Subject Rights

a. During the applicable Term, ERP Maestro, Inc. will, in a manner consistent with the functionality of the Services, enable Client to access, rectify and restrict processing of Client Data, including via the deletion functionality provided by ERP Maestro, Inc. as described in this DPA and to export Client Data.

b. ERP Maestro, Inc. agrees and warrants that it will deal promptly and properly with all inquiries from the Client relating to its processing of the Client personal data and to abide by the advice of the supervisory authorities with regard to the processing of the Client personal data.

c. Client agrees that (taking into account the nature of the processing of Client Personal Data) ERP Maestro, Inc. will assist Client in fulfilling any obligation to respond to requests by data subjects, including if applicable Client's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by complying with the GDPR obligatory requirements.

22. Transfers of Data Out of the EU/EEA

a. Client agrees that ERP Maestro, Inc. may store and process Client Data in the United States and any other country in which ERP Maestro, Inc. or any of its Subprocessors maintains facilities.

b. If the storage and/or processing of Client Personal Data involves transfers of Client Personal Data out of the EU/EEA and the European Data Protection Legislation applies to the transfers of such data ("Transferred Personal Data"), ERP Maestro, Inc. may enter into Standard Contract Clauses with Subprocessors as provided by the respective Subprocessors and that the transfers are made in accordance with such Standard Contract Clauses. Taking into account the state of technologies and the extensive use of internet in acquiring some services, Client agrees that ERP Maestro, Inc. may also accept Subprocessors' Terms of Use or any equivalent or alternative, provided by Subprocessors via their websites.

c. In respect of Transferred Personal Data, shall be considered as a contractual obligation of ERP Maestro, Inc. in fulfilling ERP Maestro, Inc. obligation to provide the Services and more specifically as a Client's instruction in the meaning of GDPR.

d. Whenever ERP Maestro, Inc. has entered into Standard Contract Clauses, ERP Maestro, Inc. will ensure that any disclosure of Client's personal data, and any notifications relating to any such disclosures, will be made in accordance with such Standard Contract Clauses, the requirements of applicable European Data Protection Legislation and the binding decisions of the European Commission and the European Court of Justice.

e. In respect of Transferred Personal Data, Client agrees that any such Transfer of Data, executed in compliance with this Section 22, shall be considered as suitable guarantee and an effective legal tool for personal data protection.

23. Subprocessors

a. Client generally authorizes the engagement of any other third parties as Subprocessors **("Third Party Subprocessors")**.

b. Information about the ERP Maestro, Inc. Subprocessors is available in Appendix 1 below and may be updated by ERP Maestro, Inc. from time to time.

c. When engaging any Subprocessor, ERP Maestro, Inc. will ensure via a written contract or another suitable electronic form that: (i) the Subprocessor only accesses and uses Client Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with any Standard Contract Clauses entered into by ERP Maestro, Inc. ; and (ii) if the GDPR applies to the processing of Client Personal Data, the data protection obligations set out in Article 28(3) of the GDPR, as required by the GDPR, are imposed on the Subprocessor.

d. Subprocessor remain fully liable for all obligations subcontracted to them and all acts and omissions of the Subprocessor except for all cases when the GDPR transfers the liability for Subprocessors to ERP Maestro, Inc. in its capacity of a processor.

e. When any Additional service is engaged via a Third Party Subprocessor during the applicable Term, ERP Maestro, Inc. will inform the Client of the engagement either by sending a Newsletter or an email to the Client Email Address or via the Admin Console.

f. Client may object to any new Third Party Subprocessor by terminating the applicable Agreement or the Service, provided by the Subprocessor immediately upon written notice to ERP Maestro, Inc., on condition that

Client provides such notice within 30 days of being informed of the engagement of the Subprocessor. This termination right is Client's sole and exclusive remedy if Client objects to any new Third Party Subprocessor.

24. Records

a. Client acknowledges that ERP Maestro, Inc. is required under the GDPR to: (a) collect and maintain records of certain information, Including the name and contact details of each processor and/or controller on behalf of which ERP Maestro, Inc. is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly, if the GDPR applies to the processing of Client Personal Data, Client will, where requested, provide such information to ERP Maestro, Inc. and will ensure that all information provided is kept accurate and up-to-date.

25. Liability

a. Nothing in this DPA will affect the remaining terms of the applicable Agreement relating to liability (including any specific exclusions from any limitation of liability).

26. Effect of Addendum

a. To the extent of any conflict or inconsistency between the terms of this Data Processing Addendum and the remainder of the applicable Agreement, the terms of this Data Processing Addendum will govern. For clarity, this Data Processing Addendum will, as from the Effective Date be effective and replace any previously applicable data processing provisions.

b. Effective Date means, as applicable: (a) 23 January 2019, if Client clicked to accept or the parties otherwise agreed to this Data Processing Addendum in respect of the applicable Agreement prior to or on such date; or (b) the date on which Client clicked to accept or the parties otherwise agreed to this Data Processing Addendum in respect of the applicable Agreement, if such date is after 23 January 2019.

c. This Data Processing Addendum will take effect on the Effective Date and, notwithstanding expiry of the Term, remain in effect until, and automatically expire upon, deletion of all Client Data by ERP Maestro, Inc.

27. Applicable law

a. This DPA shall be governed by the law of the United States. The place of jurisdiction for all disputes regarding this DPA shall be Broward County Florida USA except as otherwise stipulated by applicable data protection law.

Appendix 1: SUBPROCESSORS

1. For providing quality services to the Client ERP Maestro, Inc. engages a number of Subprocessors, carefully selected according to their capacity for Client personal data protection and processing in compliance with ERP Maestro, Inc.'s obligations under this DPA and the GDPR.
2. All Subprocessors, situated out of EU, whose services require transfer of personal data out of EU, shall be compliant with the requirements of Section 22. Transfers of Data Out of the EU/EEA.
3. ERP Maestro, Inc. uses as Subprocessors and Client personal data may be transferred to the providers of the following services:
    a. Customer relationship management (Salesforce);
    b. Email automation software (Pardot);
    c. Email server (Microsoft Office 365);
    d. Hosting services (Microsoft Azure);
    e. Survey software (SurveyMonkey).
4. ERP Maestro, Inc. may replace its Subprocessors from time to time following above rules of strict selection. Updated information about the list of current Subprocessors may be found at all times here on our website and we may inform you about such updates via our monthly newsletters.
5. The right to object or terminate the agreement is included in Sec. 23f f: Client may object to any new Third Party Subprocessor by terminating the applicable Agreement or the Service, provided by the Subprocessor immediately upon written notice to ERP Maestro, Inc., on condition that Client provides such notice within 30 days of being informed of the engagement of the Subprocessor. This termination right is Client's sole and exclusive remedy if Client objects to any new Third Party Subprocessor.

Appendix 2: DESCRIPTION OF THE TECHNICAL AND ORGANISATIONAL SECURITY MEASURES IMPLEMENTED BY ERP Maestro, Inc.:

SECURITY AREAS	SECURITY MEASURES FOR PERSONAL DATA PROTECTION
NETWORK AND SYSTEMS SECURITY	Firewall and router configurations have to be set-up, in order to restrict the traffic, inbound and outbound, from "untrusted" networks (including wireless) and hosts. Deny all other traffic except, for protocols necessary for the personal data environment (PDE).
	Application firewalls have to be set-up in front of web servers belonging to PDE, in order to verify and validate the traffic which is directed to the server. Any unauthorized service or traffic should be blocked, and an alert should be generated.

	Production (real) data should only be allowed in production environments. Upon exception and with all necessary approvals, QA environments may process (real) personal data only to the extent that they are protected as production environments. The environment of testing and development, as well as pre-production environments must use either anonymized or synthetic data.
	Standard hardening configuration templates have to be developed for databases, applications, operating systems and applications containing personal data.
DATA SECURITY	Personal data retention time must be limited to the extent which is necessary for each single processing activity, albeit in compliance with legal and/or regulatory (retention) obligations.
	Personal data has to be made unreadable (e.g. leveraging on encryption), when stored on portable digital media, backup media, log files.
	Strong cryptography and security protocols have to be implemented, in order to protect personal data during the transmission over open, public or untrusted networks.
	In case the channel encryption is not possible, files and attachments containing personal data have to be protected by means of encryption whenever they are transmitted over open, public or untrusted networks.
	Security tools should be used, to monitor and control the flow of personal data through endpoints and towards external networks.
	Databases/data storages encryption should be based upon a proper classification of assets in scope, according to the level of criticality.
	Media containing personal data must be protected against unauthorized access, through adequate physical (e.g. lock) and logical (e.g. encryption, access control, etc.) security measures.
	Upon return and/or dismissal of ICT assets and resources, secure clean-up procedures (e.g. wiping) should be put in place, in order to remove all personal data and/or securely overwrite prior to disposal or re-use.
	Paper documents or magnetic/optical media (e.g.: hard disks, DVDs, CDs, smart cards, USB flash drives) have to be destroyed or rendered unusable to ensure that the data and information they contain cannot be reconstructed and/or used (even partially) by unauthorized Third Parties. Paper documents have to be physically destroyed before being trashed, through specific shredder devices.
	Employees must be adequately educated and trained on the correct rules of conduct to be adopted for the protection of personal data contained in paper documents (example: in case of removal from the workstation make sure that nobody can access confidential information, protect the original documents and the photocopies from theft or unauthorized use, keep the documentation in drawers and closets locked at the end of the working session)

DATA AVAILABILITY	Proper procedures should be put in place in order to restore the availability of personal data (as a right of the data subject) in a timely manner. Back-up procedures should ensure copies of personal data at least weekly.
IDENTITY AND ACCESS MANAGEMENT	Access authorization to production environments containing personal data should be given according to the "need to know" and “least privilege” principles.
	Policies and procedures must be implemented to ensure the proper identification of users and administrators accessing system components managing personal data. All users should be assigned with a unique user name before allowing them to access system components or personal data.
	Individual remote administrative accesses to systems managing personal data have to be protected, by means of an authentication mechanism requiring password changes every 90 days. Additionally, password vaulting tools should be evaluated in order to increase credentials' security.
	Passwords for systems and devices managing personal data must contain at least 8 digits, not easily attributable to the user, and they must be changed at least every 3 months.
	System resources and access right must be assigned to user accounts, where user accounts are assigned to unique users.
	All accesses to databases containing personal data should be protected/controlled as follows: - Application credentials to access databases cannot be used by individual users or other non-application processes - Such application/system user credentials must be appropriately protected against potential misuse. - Access must be granted only to the personnel who really needs it for the performance of own job/tasks (need to know principles) - A formal user registration and de-registration process should be implemented to enable assignment of access rights to manage personal data.
	Number of personal data repositories (databases, files, copies, archives) should be kept to an absolute minimum, avoiding unnecessary duplication. Instead of duplication, preference should be given to pseudonymized databases, that perform look-ups into master repositories for specific personal data, if, and when needed.
	Visibility of personal data must be limited to the sole set of information which is necessary for the single processing activities. No unnecessary personal data should be made available to users.
	Users’ access rights to personal data should be reviewed/re-certified at regular intervals and, in any case, at least annually – as per the regular Identity and Access Management process.
	Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged onto the

	machine without administrative privileges, the administrator should gain administrative privileges.
LOGGING AND MONITORING	Access to production environments containing personal data - and where technically possible access to personal data - should be monitored and logged, in order to precisely record the link between access and individual user accessing personal data
ORGANISATION AND HUMAN SECURITY	Adequate procedures should be put in place to ensure the continuous availability of personal data: back-up personnel should be identified to ensure the continuity of the service to the data subject willing to access own personal data.
	A formal security awareness program has to be implemented, to make all personnel aware of policy and procedures related to personal data security. Periodic tests or simulations may be performed, to assess whether employees click on a link from suspicious e-mail or provide personal/sensitive information without following appropriate security procedures to verify the reliability of the source. As a consequence, targeted training should be provided to those employees falling victim to the test.
	Clear contractual agreements have to be signed-off with service providers, in order to state their responsibility for the security of personal data they process/store/transmit on behalf of the Data Controller.
	Employees responsibilities and duties on the confidentiality of personal data should be clearly stated as valid also after the termination or change of employment.
	Personal data must not be copied on removable media, except from those media expressly authorized by the Processor for specific tasks.
DATA PROTECTION BY DESIGN	Processes and tools for the Secure Software Development Lifecycle (SDLC) have to be integrated with appropriate security check/controls and requirements, in order to ensure that new ICT software/applications are designed and developed taking into consideration the requirements of embedded security.
	Processes of ICT Change Management have to be integrated with appropriate security check/controls and requirements, in order to ensure the continuous protection of ICT software/applications in place, upon relevant changes.
PERSONAL DATA BREACH NOTIFICATION	Processes and tools for Incident Management have to be properly implemented and/or improved, in order to enable the detection and classification of personal data breaches so that they are correctly communicated to the Controller within the terms established in the paragraph “Notification obligation and Security Breach “.
	A register of personal data breaches should be created and maintained.