workbox

TERMS OF DATA PROCESSING AND SECURITY

Last updated on [7/11/2018].

The customer agreeing to these terms ("Customer"), and Woodshed LLC (doing business as Workbox), or any other entity that directly or indirectly controls, is controlled by, or is under common control with Woodshed LLC (as applicable, "Workbox"), have entered into an agreement under which Workbox has agreed to provide Workbox and ArchiveIt (as described at https://www.workbox.app/terms/services) and related technical support to Customer (as amended from time to time, the "Agreement").

These Data Processing and Security Terms, including their appendices (the "Terms") will be effective and replace any previously applicable data processing and security terms as from the Terms Effective Date (as defined below).

These Terms supplement the Agreement.

1. Introduction

These Terms reflect the parties' agreement with respect to the terms governing the processing and security of Customer Data under the Agreement.

2. Definitions

2.1 Capitalized terms used but not defined in these Terms have the meanings set out in the Agreement. In these Terms, unless stated otherwise:

Additional Security Controls means security resources, features, functionality and/or controls that Customer may use at its option and/or as it determines, including the Admin Console and other features and/or functionality of the Services such as encryption, logging and monitoring, identity and access management, security scanning, and firewalls. Agreed Liability Cap means the maximum monetary or payment-based amount at which a party's liability is capped under the Agreement, either per annual period or event giving rise to liability, as applicable. Alternative Transfer Solution means a solution, other than the Model Contract Clauses, that enables the lawful transfer of personal data to a third country in accordance with Article 45 or 46 of the GDPR (for example, the EU-U.S. Privacy Shield). Audited Services means the Services indicated as being in-scope for the relevant certification or report at https://www.workbox.app/security/compliance/services-in-scope, as may be updated by Workbox from time to time, provided that Workbox may only remove a Deprecation Policy Service from such URL if that Service has been discontinued in accordance with the Deprecation Policy. Customer Data has the meaning given in the Agreement or, if no such meaning is given, means data provided by or on behalf of Customer or Customer End Users via the Services under the Account. Customer End Users has the meaning given in the Agreement or, if not such meaning is given, has the meaning given to "End Users"

in the Agreement. Customer Personal Data means the personal data contained within the Customer Data. Data Incident means a breach of Workbox's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Workbox. "Data Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems. Deprecation Policy Service means a Service identified at https://wwww.workbox.app/terms/deprecation. EEA means the European Economic Area. European Data Protection Legislation means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland). 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. Workbox's Third Party Auditor means a Workbox-appointed, qualified and independent third party auditor, whose then-current identity Workbox will disclose to Customer. ISO 27001 Certification means an ISO/IEC 27001:2013 certification or a comparable certification for the Audited Services. ISO 27017 Certification means an ISO/IEC 27017:2015 certification or a comparable certification for the Audited Services. ISO 27018 Certification means an ISO/IEC 27018:2014 certification or a comparable certification for the Audited Services. Model Contract Clauses or MCCs mean 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. Non-European Data Protection Legislation means data protection or privacy legislation in force outside the European Economic Area and Switzerland. Notification Email Address means the email address(es) designated by Customer in the Admin Console, or in the Order Form or Ordering Document (as applicable), to receive certain notifications from Workbox. Security Documentation means all documents and information made available by Workbox under Section 7.5.1 (Reviews of Security Documentation). Security Measures has the meaning given in Section 7.1.1 (Workbox's Security Measures). Subprocessors means third parties authorized under these Terms to have logical access to and process Customer Data in order to provide parts of the Services. Term means the period from the Terms Effective Date until the end of Workbox's provision of the Services, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which Workbox may continue providing the Services for transitional purposes. Terms Effective Date means the date on which Customer accepted, or the parties otherwise agreed to, these Terms.

2.2 The terms "personal data", "data subject", "processing", "controller", "processor" and "supervisory authority" as used in these Terms have the meanings given in the GDPR, and the terms "data importer" and "data exporter" have the meanings given in the Model Contract Clauses, in each case irrespective of whether the European Data Protection Legislation or Non-European Data Protection Legislation applies.

3. Duration of these Terms

These Terms will take effect on the Terms Effective Date and, notwithstanding expiry of the Term, will remain in effect until, and automatically expire upon, deletion of all Customer Data by Workbox as described in these Terms.

4. Scope of Data Protection Legislation

4.1 Application of European Legislation. The parties acknowledge and agree that the European Data Protection Legislation will apply to the processing of Customer Personal Data if, for example: the processing is carried out in the context of the activities of an establishment of Customer in the territory of the EEA; and/or the Customer Personal Data is personal data relating to data subjects who are in the EEA and the processing relates to the offering to them of goods or services in the EEA or the monitoring of their behaviour in the EEA.

4.2 Application of Non-European Legislation. The parties acknowledge and agree that Non-European Data Protection Legislation may also apply to the processing of Customer Personal Data.

4.3 Application of Terms. Except to the extent these Terms state otherwise, these Terms will apply irrespective of whether the European Data Protection Legislation or Non-European Data Protection Legislation applies to the processing of Customer Personal Data.

5. Processing of Data

5.1 Roles and Regulatory Compliance; Authorization.

5.1.1 Processor and Controller Responsibilities. If the European Data Protection Legislation applies to the processing of Customer Personal Data, the parties acknowledge and agree that: the subject matter and details of the processing are described in Appendix 1; Workbox is a processor of that Customer Personal Data under the European Data Protection Legislation; Customer is a controller or processor, as applicable, of that Customer Personal Data under European Data Protection Legislation; and each party will comply with the obligations applicable to it under the European Data Protection Legislation with respect to the processing of that Customer Personal Data.

5.1.2 Authorization by Third Party Controller. If the European Data Protection Legislation applies to the processing of Customer Personal Data and Customer is a processor, Customer warrants to Workbox that Customer's instructions and actions with respect to that Customer Personal Data, including its appointment of Workbox as another processor, have been authorized by the relevant controller.

5.1.3 Responsibilities under Non-European Legislation. If Non-European Data Protection Legislation applies to either party's processing of Customer Personal Data, the parties acknowledge and agree that the relevant party will comply with any obligations applicable to it under that legislation with respect to the processing of that Customer Personal Data.

5.2 Scope of Processing.

5.2.1 Customer's Instructions. By entering into these Terms, Customer instructs Workbox to process Customer Personal Data only in accordance with applicable law: (a) to provide the Services; (b) as further specified via Customer's use of the Services (including the Admin Console and other functionality of the Services); (c) as documented in the form of the Agreement, including these Terms; and (d) as further documented in any other written instructions given by Customer and acknowledged by Workbox as constituting instructions for purposes of these Terms.

5.2.2 Workbox's Compliance with Instructions. Workbox will comply with the instructions described in Section 5.2.1 (Customer's Instructions) (including with regard to data transfers) unless EU or EU Member State law to which Workbox is subject requires other processing of Customer Personal Data by Workbox, in which case Workbox will inform Customer (unless that law prohibits Workbox from doing so on important grounds of public interest) via the Notification Email Address.

6. Data Deletion

6.1 Deletion by Customer. Workbox will enable Customer to delete Customer Data during the Term in a manner consistent with the functionality of the Services. If Customer uses the Services to delete any Customer Data during the Term and that Customer Data cannot be recovered by Customer, this use will constitute an instruction to Workbox to delete the relevant Customer Data from Workbox's systems in accordance with applicable law. Workbox will comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days, unless EU or EU Member State law requires storage.

6.2 Deletion on Termination. On expiry of the Term, Customer instructs Workbox to delete all Customer Data (including existing copies) from Workbox's systems in accordance with applicable law. Workbox will, after a recovery period of up to 30 days following such expiry, comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days, unless EU or EU Member State law requires storage. Without prejudice to Section 9.1 (Access; Rectification; Restricted Processing; Portability), Customer acknowledges and agrees that Customer will be responsible for exporting, before the Term expires, any Customer Data it wishes to retain afterwards.

7. Data Security

7.1 Workbox's Security Measures, Controls and Assistance.

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

7.1.2 Security Compliance by Workbox Staff. Workbox will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.1.3 Additional Security Controls. In addition to the Security Measures, Workbox will make the Additional Security Controls available to: (a) allow Customer to take steps to secure Customer Data; and (b) provide Customer with information about securing, accessing and using Customer Data.

7.1.4 Workbox's Security Assistance. Customer agrees that Workbox will (taking into account the nature of the processing of Customer Personal Data and the information available to Workbox) assist Customer in ensuring compliance with any of Customer's obligations in respect of security of personal data and personal data breaches, including if applicable Customer's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by: implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Workbox's Security Measures); making the Additional Security Controls available to Customer in accordance with Section 7.1.3 (Additional Security Controls); complying with the terms of Section 7.2 (Data Incidents); and providing Customer with the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation) and the information contained in the Agreement including these Terms.

7.2 Data Incidents

7.2.1 Incident Notification. If Workbox becomes aware of a Data Incident, Workbox will: (a) notify Customer of the Data Incident promptly and without undue delay after becoming aware of the Data Incident; and (b) promptly take reasonable steps to minimize harm and secure Customer Data.

7.2.2 Details of Data Incident. Notifications made pursuant to this section will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps Workbox recommends Customer take to address the Data Incident.

7.2.3 Delivery of Notification. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address or, at Workbox's discretion, by direct communication (for example, by phone call or an in-person meeting). Customer is solely responsible for ensuring that the Notification Email Address is current and valid.

7.2.4 No Assessment of Customer Data by Workbox. Workbox will not assess the contents of Customer Data in order to identify information subject to any specific legal requirements. Without prejudice to Workbox's obligations under this Section 7.2 (Data Incidents), Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Data Incident(s).

7.2.5 No Acknowledgement of Fault by Workbox. Workbox's notification of or response to a Data Incident under this Section 7.2 (Data Incidents) will not be construed as an acknowledgement by Workbox of any fault or liability with respect to the Data Incident.

7.3 Customer's Security Responsibilities and Assessment.

7.3.1 Customer's Security Responsibilities. Customer agrees that, without prejudice to Workbox's obligations under Section 7.1 (Workbox's Security Measures, Controls and Assistance) and Section 7.2 (Data Incidents):

Customer is solely responsible for its use of the Services, including: making appropriate use of the Services and the Additional Security Controls to ensure a level of security appropriate to the risk in respect of the Customer Data; securing the account authentication credentials, systems and devices Customer uses to access the Services; backing up its Customer Data as appropriate; and Workbox has no obligation to protect copies of Customer Data that Customer elects to store or transfer outside of Workbox's and its Subprocessors' systems (for example, offline or on-premises storage), or to protect Customer Data by implementing or maintaining Additional Security Controls except to the extent Customer has opted to use them.

7.3.2 Customer's Security Assessment. Customer is solely responsible for reviewing the Security Documentation and evaluating for itself whether the Services, the Security Measures, the Additional Security Controls and Workbox's commitments under this Section 7 (Data Security) will meet Customer's needs, including with respect to any security obligations of Customer under the European Data Protection Legislation and/or Non-European Data Protection Legislation, as applicable. Customer

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 Customer Personal Data as well as the risks to individuals) the Security Measures implemented and maintained by Workbox as set out in Section 7.1.1 (Workbox's Security Measures) provide a level of security appropriate to the risk in respect of the Customer Data.

7.4 Security Certifications and Reports. Workbox will continue to maintain certifications and provide security reports as appropriate to maintain obligations under these Terms.

7.5 Reviews and Audits of Compliance

7.5.1 Reviews of Security Documentation. In addition to the information contained in the Agreement (including these Terms), Workbox will make available for review by Customer any relevant security documentation that demonstrate compliance by Workbox with its obligations under these Terms, following a request by Customer in accordance with Section 7.5.3.

7.5.2 Customer's Audit Rights. If the European Data Protection Legislation applies to the processing of Customer Personal Data, Workbox will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Workbox's compliance with its obligations under these Terms in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits). Workbox will contribute to such audits as described in Section 7.4 (Security Certifications and Reports) and this Section 7.5 (Reviews and Audits of Compliance). If Customer has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data Out of the EEA), Workbox will, without prejudice to any audit rights of a supervisory authority under such Model Contract Clauses, allow Customer or an independent auditor appointed by Customer to conduct audits as described in the Model Contract Clauses in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits). Customer may also conduct an audit to verify Workbox's compliance with its obligations under these Terms by reviewing the relevant Security Documentation.

7.5.3 Additional Business Terms for Reviews and Audits. Customer must send any requests for reviews or audits under Section 7.5.2 to Workbox as described in Section 12 (Cloud Data Protection Team; Processing Records). Following receipt by Workbox of a request under Section 7.5.3, Workbox and Customer will discuss and agree in advance on: (i) the reasonable date(s) of and security and confidentiality controls applicable to any review of documentations under Section 7.5.1; and (ii) the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit under Section 7.5.2. Workbox may charge a fee (based on Workbox's reasonable costs) for any review of the documentation under Section 7.5.1 and/or audit under Section 7.5.2. Workbox will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such review or audit. Customer will be responsible for any fees charged by any auditor appointed

by Customer to execute any such audit. Workbox may object in writing to an auditor appointed by Customer to conduct any audit under Section 7.5.2 if the auditor is, in Workbox's reasonable opinion, not suitably qualified or independent, a competitor of Workbox, a competitor of Workbox Subprocessors, or otherwise manifestly unsuitable. Any such objection by Workbox will require Customer to appoint another auditor or conduct the audit itself.

7.5.4 No Modification of MCCs. Nothing in this Section 7.5 (Reviews and Audits of Compliance) varies or modifies any rights or obligations of Customer or Woodshed LLC under any Model Contract Clauses entered into as described in Section 10.2 (Transfers of Data Out of the EEA).

8. Impact Assessments and Consultations

Customer agrees that Workbox will (taking into account the nature of the processing and the information available to Workbox) assist Customer in ensuring compliance with any obligations of Customer in respect of data protection impact assessments and prior consultation, including if applicable Customer's obligations pursuant to Articles 35 and 36 of the GDPR, by: providing the Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls) and the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation); and providing the information contained in the Agreement including these Terms.

9. Data Subject Rights; Data Export

9.1 Access; Rectification; Restricted Processing; Portability. During the Term, Workbox will, in a manner consistent with the functionality of the Services, enable Customer to access, rectify and restrict processing of Customer Data, including via the deletion functionality provided by Workbox as described in Section 6.1 (Deletion by Customer), and to export Customer Data.

9.2 Data Subject Requests

9.2.1 Customer's Responsibility for Requests. During the Term, if Workbox receives any request from a data subject in relation to Customer Personal Data, Workbox will advise the data subject to submit their request to Customer and Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

9.2.2 Workbox's Data Subject Request Assistance. Customer agrees that Workbox will (taking into account the nature of the processing of Customer Personal Data) assist Customer in fulfilling any obligation to respond to requests by data subjects, including if applicable Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by: providing the Additional Security Controls in accordance with Section 7.1.3 (Additional Security

Controls); and complying with the commitments set out in Section 9.1 (Access; Rectification; Restricted Processing; Portability) and Section 9.2.1 (Customer's Responsibility for Requests).

10. Data Transfers

10.1 Data Storage and Processing Facilities Customer may select where certain Customer Data will be stored (the "Data Location Selection"), and Workbox will store it there in accordance with the Service Specific Terms. If a Data Location Selection is not covered by the Service Specific Terms (or a Data Location Selection is not made by Customer in respect of any Customer Data), Workbox may, subject to Section 10.2 (Transfers of Data Out of the EEA), store and process the relevant Customer Data anywhere Workbox or its Subprocessors maintains facilities.

10.2 Transfers of Data Out of the EEA.

10.2.1 Workbox's Transfer Obligations. If the storage and/or processing of Customer Personal Data involves transfers of Customer Personal Data out of the EEA, and the European Data Protection Legislation applies to the transfers of such data ("Transferred Personal Data"), Workbox will: if requested to do so by Customer, ensure that Woodshed LLC as the data importer of the Transferred Personal Data enters into Model Contract Clauses with Customer as the data exporter of such data, and that the transfers are made in accordance with such Model Contract Clauses; and/or offer an Alternative Transfer Solution, ensure that the transfers are made in accordance with such Alternative Transfer Solution, and make information available to Customer about such Alternative Transfer Solution.

10.2.2 Customer's Transfer Obligations. In respect of Transferred Personal Data, Customer agrees that: if under the European Data Protection Legislation Workbox reasonably requires Customer to enter into Model Contract Clauses in respect of such transfers, Customer will do so; and if under the European Data Protection Legislation Workbox reasonably requires Customer to use an Alternative Transfer Solution offered by Workbox, and reasonably requests that Customer take any action (which may include execution of documents) strictly required to give full effect to such solution, Customer will do so.

10.3 Data Center Information. Information about the locations of Workbox 3rd party data centers is available at: https://www.workbox.app/terms/datacenters (as may be updated by Workbox from time to time).

10.4 Disclosure of Confidential Information Containing Personal Data. If Customer has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data Out of the EEA), Workbox will, notwithstanding any term to the contrary in the Agreement, ensure that any disclosure of Customer's Confidential Information containing personal data, and any notifications relating to any such disclosures, will be made in accordance with such Model Contract Clauses.

11. Subprocessors

11.1 Consent to Subprocessor Engagement. Customer specifically authorizes the engagement as Subprocessors of: (a) those entities listed as of the Terms Effective Date at the URL specified in Section 11.2 (Information about Subprocessors); and (b) all other Workbox Affiliates from time to time. In addition, Customer generally authorizes the engagement as Subprocessors of any other third parties ("New Third Party Subprocessors"). If Customer has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data Out of the EEA), the above authorizations will constitute Customer's prior written consent to the subcontracting by Woodshed LLC of the processing of Customer Data if such consent is required under the Model Contract Clauses.

11.2 Information about Subprocessors. Information about Subprocessors, including their functions and locations, is available at:https://www.workbox.app/terms/third-party-suppliers (as may be updated by Workbox from time to time in accordance with these Terms).

11.3 Requirements for Subprocessor Engagement. When engaging any Subprocessor, Workbox will: ensure via a written contract that: the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including these Terms) and any Model Contract Clauses entered into or Alternative Transfer Solution adopted by Workbox as described in Section 10.2 (Transfers of Data Out of the EEA); and if the GDPR applies to the processing of Customer Personal Data, the data protection obligations set out in Article 28(3) of the GDPR, as described in these Terms, are imposed on the Subprocessor; and remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

11.4 Opportunity to Object to Subprocessor Changes. When any New Third Party Subprocessor is engaged during the Term, Workbox will, at least 30 days before the New Third Party Subprocessor processes any Customer Data, inform Customer of the engagement (including the name and location of the relevant subprocessor and the activities it will perform) by sending an email to the Notification Email Address. Customer may object to any New Third Party Subprocessor by terminating the Agreement immediately upon written notice to Workbox, on condition that Customer provides such notice within 90 days of being informed of the engagement of the subprocessor as described in Section 11.4(a). This termination right is Customer's sole and exclusive remedy if Customer objects to any New Third Party Subprocessor.

12. Cloud Data Protection Team; Processing Records

12.1 Workbox's Cloud Data Protection Team. Workbox's Cloud Data Protection Team can be contacted at contact@workbox.io (and/or via such other means as Workbox may provide from time to time).

12.2 Workbox's Processing Records. Customer acknowledges that Workbox 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 Workbox 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 Customer Personal Data, Customer will, where requested, provide such information to Workbox via the Admin Console or other means provided by Workbox, and will use the Admin Console or such other means to ensure that all information provided is kept accurate and up-to-date.

13. Liability

13.1 Liability Cap. If Model Contract Clauses have been entered into as described in Section 10.2 (Transfers of Data Out of the EEA), the total combined liability of either party and its Affiliates towards the other party and its Affiliates under or in connection with the Agreement and such Model Contract Clauses combined will be limited to the Agreed Liability Cap for the relevant party, subject to Section 13.2 (Liability Cap Exclusions).

13.2 Liability Cap Exclusions. Nothing in Section 13.1 (Liability Cap) will affect the remaining terms of the Agreement relating to liability (including any specific exclusions from any limitation of liability).

14. Third Party Beneficiary

Notwithstanding anything to the contrary in the Agreement, where Woodshed LLC is not a party to the Agreement, Woodshed LLC will be a third party beneficiary of Section 7.5 (Reviews and Audits of Compliance), Section 11.1 (Consent to Subprocessor Engagement) and Section 13 (Liability) of these Terms.

15. Effect of These Terms

Notwithstanding anything to the contrary in the Agreement, to the extent of any conflict or inconsistency between these Terms and the remaining terms of the Agreement, these Terms will govern.