Exhibit C

Data Processing Addendum (US Customers)

Last modified March 13, 2025

This Data Processing Addendum ("**DPA**") is incorporated into the agreement(s) under which Mark43 has agreed to provide Software and Services to Subscriber (the "**Agreement**").

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

1. **Definitions.** For purposes of this DPA, "**Subprocessor**" means a Mark43 Affiliate or other third party engaged by Mark43 for the purpose of hosting, storing or otherwise processing Subscriber Data as authorized by the Agreement or otherwise in writing by Subscriber. "**Integrated Application**" shall have the meaning ascribed to it in the Agreement and if not therein defined, shall mean a third-party product, service, database, or application that will be installed, linked or enabled by Mark43 or Subscriber for use in connection with the SaaS Services. Terms not otherwise defined in this DPA have the meaning set out in the Agreement.

2. **Subscriber Data.** The obligations in this Schedule apply to Subscriber Data in the custody or control of Mark43 and its Subprocessors. They do not apply to Subscriber Data in the custody or control of any other party, including Subscriber Data under Subscriber's custody or control outside of the Services or Subscriber Data maintained by the provider of an Integrated Application or transmitted or accessed on or through an Integrated Application.

3. **Disclosure.** Mark43 will not disclose Subscriber Data to any third party except: (i) to Authorized Users; (ii) as permitted under the Agreement; (iii) to Mark43 Vendors and its Subprocessors, provided that each Mark43 Vendor and Subprocessor agrees to protect Subscriber Data in a manner substantially in accordance with this DPA; or as provided by this DPA with respect to any Disclosure Request. Notwithstanding the foregoing or anything in this DPA or elsewhere in the Agreement to the contrary, Subscriber acknowledges and agrees that (a) Mark43 utilizes major providers of cloud-based services for processing certain Subscriber Data through the Services (each, a "**Cloud Provider**"), (b) each Cloud Provider has its own data protection practices that are applicable to its delivery of services to its customers, and (c) Cloud Providers will not agree to separate data protection practices on a customer-

by-customer basis; therefore, Cloud Providers will not be required to comply with the obligations in this DPA to the extent that they are inconsistent with each Cloud Provider's own data protection practices, but Mark43 will use reasonable efforts to assess that each Cloud Provider complies with its own data protection practices, which may include periodic examination of SOC 2 reports or comparable reports made available by Cloud Provider.

4. **Information Security Program.** Mark43 will implement and maintain a written information security program that contains reasonable administrative, technical and physical safeguards intended to protect Subscriber Data from unauthorized access, disclosure, use, modification, loss or destruction.

5. **Access.** Mark43 will maintain appropriate access controls to Subscriber Data, including limiting access to Subscriber Data only to personnel who require such access in order for Mark43 to provide Services to Subscriber or to otherwise exercise Mark43's rights or perform Mark43's obligations under the Agreement. Mark43 will require its personnel to protect Subscriber Data in accordance with the requirements of this DPA and will provide its personnel with appropriate information security training.

6. **Information Security.**

    1. Mark43 maintains its information security program and applicable safeguards at all Mark43 sites at which an information system that stores or otherwise processes Subscriber Data is located.

    2. Mark43 maintains network security using commercially available equipment and industry standard techniques, including firewalls, router access control lists, intrusion detection and/or prevention systems, penetration testing, vulnerability scanning, and patch management tools.

    3. Mark43 will encrypt, using industry-standard encryption tools, all Subscriber Data that Mark43: (i) transmits or sends wirelessly or across public networks; (ii) stores on laptops or removable storage media; and (iii) stores on portable devices. Mark43 will safeguard the confidentiality and availability of all encryption keys associated with encrypted Subscriber Data.

    4. Mark43 installs and maintains endpoint security measures such as anti-virus and malware protection software intended to protect Subscriber Data from malicious code.

5. Mark43 undertakes appropriate logging and monitoring to enable recording of information security-related actions and identification of anomalous events.
6. Mark43 develops software used to deliver the Services in accordance with secure software development principles.

7. **Security Incident Management.** Unless otherwise prohibited by law, Mark43 will notify Subscriber promptly (and in any event within seventy-two (72) hours) in the event Mark43 reasonably believes that there has been any unauthorized access, acquisition, disclosure, use, modification, loss or destruction of Subscriber Data ("**Security Incident**"). Mark43 will promptly investigate the Security Incident, will take necessary steps to eliminate or contain the exposure of Subscriber Data, and will keep Subscriber informed of the status of the Security Incident. Mark43 will provide reasonable assistance and cooperation requested by Subscriber or Subscriber's designated representatives to correct, remediate, or investigate the Security Incident or to mitigate potential damage resulting from it, including any notification that Subscriber may determine appropriate to send to affected individuals, regulators or third parties.
8. **Business Continuity.** Mark43 implements appropriate disaster recovery and business continuity plans and reviews and updates such plans regularly. Back-up copies of critical business information and software are created regularly and tested to verify their integrity.
9. **Audits.** Upon Subscriber's request, Mark43 will make available to Subscriber up to once per year a copy of a third-party assessment, such as a SOC 2 or comparable report ("**Third-Party Report**"), if Mark43 has obtained such a Third-Party Report for the Services; or if Mark43 has not obtained a Third-Party Report for the Services, Subscriber may provide to Mark43 a security assessment questionnaire related to the Services, which Mark43 will complete within 30 days of receipt thereof. Such a questionnaire must be reasonable in scope and may include questions seeking verification of compliance with the terms and conditions of this DPA. All Third-Party Reports or information accessed by or otherwise disclosed to Subscriber in connection with any such review will be considered Confidential Information of Mark43.
10. **Return/Disposal.** Upon termination or expiration of the Agreement, Mark43 will cease handling Subscriber Data and will take reasonable steps to permanently delete Subscriber Data within thirty (30) days of delivery of such data to Subscriber

pursuant to the Agreement. If Mark43 has any legal obligation to retain any Subscriber Data, it will comply with relevant Applicable Laws and destroy such Subscriber Data in accordance with this DPA as soon as practicable after that legally required retention period has ended. If Mark43 disposes of any paper, electronic or other record containing Subscriber Data, Mark43 will take all reasonable steps to do so by: (a) shredding; (b) permanently erasing and deleting; (c) degaussing; or (d) otherwise modifying Subscriber Data in such records to make it unreadable, unreconstructable and indecipherable.

11. **Location of Subscriber Data.** Subscriber Data stored or transmitted through the SaaS Services in Subscriber's user accounts shall be hosted by a Cloud Provider in the United States.