LEGAL · DATA PROCESSING

Data Processing Addendum

Effective date: November 1, 2025 · PestMetry, Inc.

This Data Processing Addendum ("DPA") supplements and forms part of the agreement between PestMetry ("PestMetry," "we," "us," or "our") and the customer identified in the underlying subscription, order form, or Terms of Service ("Customer," "you," or "your") (collectively, the "Agreement") governing Customer's use of the PestMetry warehouse pest management and sanitation intelligence platform and related services (the "Services"). This DPA reflects the parties' agreement regarding the Processing of Personal Data by PestMetry on behalf of Customer in connection with the Services. In the event of any conflict between this DPA and the Agreement, this DPA will control with respect to Processing of Personal Data.

1. Definitions

Capitalized terms not defined here have the meanings given in the Agreement or in Data Protection Laws. For purposes of this DPA:

- **"Data Protection Laws"** means all privacy and data protection laws applicable to a party's Processing of Personal Data under this DPA, including, as applicable, the EU General Data Protection Regulation 2016/679 ("GDPR"), the UK Data Protection Act 2018 and UK GDPR, the Swiss Federal Act on Data Protection ("FADP"), the California Consumer Privacy Act as amended by the CPRA ("CCPA"), and other US state comprehensive privacy laws (collectively, "US State Privacy Laws").
- **"Personal Data"** means any information relating to an identified or identifiable natural person that is Processed by PestMetry on behalf of Customer in connection with the Services, and includes "personal information" as defined under US State Privacy Laws.
- **"Processing"** means any operation performed on Personal Data, whether or not by automated means, including collection, storage, use, disclosure, or deletion.
- **"Controller," "Processor," "Data Subject,"** and **"Supervisory Authority"** have the meanings in the GDPR (or their equivalents under other Data Protection Laws, including "Business," "Service Provider," and "Consumer" under the CCPA).
- **"Sub-processor"** means any third party engaged by PestMetry that Processes Personal Data on PestMetry's behalf in the course of providing the Services.
- **"Standard Contractual Clauses"** or **"SCCs"** means the standard contractual clauses approved by the European Commission in Decision 2021/914, together with the UK International Data Transfer Addendum where applicable.

2. Roles and scope of Processing

For Personal Data Processed under the Agreement, the parties agree that Customer is the Controller (or Business) and PestMetry is the Processor (or Service Provider) acting on Customer's documented instructions. PestMetry will Process Personal Data only: (a) to provide, secure, support, monitor, troubleshoot, and improve the Services as described in the Agreement and this DPA; (b) as further instructed by Customer in writing, provided such instructions are consistent with the Agreement; and (c) as

required by applicable law, in which case PestMetry will, unless prohibited, inform Customer of that legal requirement before Processing.

PestMetry will not: (i) "sell" or "share" Personal Data as those terms are defined under US State Privacy Laws; (ii) retain, use, or disclose Personal Data for any purpose other than the business purposes specified in the Agreement, including for any commercial purpose other than providing the Services; (iii) retain, use, or disclose Personal Data outside of the direct business relationship between the parties; or (iv) combine Personal Data received from Customer with personal information received from or on behalf of any other person, except as permitted under the CCPA. PestMetry certifies that it understands and will comply with these restrictions.

The subject matter, duration, nature, and purpose of the Processing, the types of Personal Data, and the categories of Data Subjects are described in *Annex I* below.

3. Customer responsibilities

Customer represents and warrants that: (a) it has, and will maintain throughout the term of the Agreement, all necessary rights, consents, and lawful bases to authorize PestMetry to Process Personal Data in accordance with the Agreement and this DPA; (b) its instructions to PestMetry regarding Processing of Personal Data comply with Data Protection Laws; and (c) it has provided all notices required under Data Protection Laws to Data Subjects. Customer is responsible for the accuracy, quality, and legality of Personal Data and for the means by which Customer acquired that data.

4. Confidentiality and personnel

PestMetry will ensure that personnel authorized to Process Personal Data are bound by written or statutory obligations of confidentiality, have received appropriate training on their responsibilities under Data Protection Laws, and access Personal Data only on a need-to-know basis to perform their duties.

5. Security measures

PestMetry will implement and maintain appropriate technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing. Current measures are described in *Annex II* below and include, at a minimum: encryption in transit and at rest, role-based access controls, least-privilege administrative access, network segregation, logging and monitoring, secure development practices, vulnerability management, background checks for personnel with access to production systems, business continuity and disaster recovery, and a documented incident response process.

6. Sub-processors

Customer provides general written authorization for PestMetry to engage Sub-processors to Process Personal Data in connection with the Services. PestMetry will: (a) enter into a written agreement with each Sub-processor imposing data protection obligations that are materially no less protective than those in this DPA; (b) remain responsible for the acts and omissions of its Sub-processors to the same extent PestMetry would be liable if performing the Sub-processor's services directly; and (c) maintain a current list of Sub-processors at pestmetry.com/legal/subprocessors.

PestMetry will provide reasonable prior notice (which may be given by updating the Sub-processor page or by email to Customer's designated contact) of the addition or replacement of any Sub-processor. If Customer has a reasonable, good-faith objection based on data protection grounds, Customer may notify PestMetry within thirty (30) days of such notice. The parties will work in good faith to resolve the objection; if the parties cannot agree on a resolution, Customer may, as its sole and exclusive remedy, terminate the affected portion of the Services on written notice.

7. International data transfers

To the extent that PestMetry's Processing of Personal Data involves a transfer of Personal Data originating in the European Economic Area, the United Kingdom, or Switzerland to a country not recognized as providing an adequate level of protection, such transfers will be governed by the Standard Contractual Clauses, which are hereby incorporated by reference. For transfers from Customer (as data exporter) to PestMetry (as data importer), Module Two (Controller to Processor) applies; for onward transfers by PestMetry to Sub-processors, Module Three (Processor to Processor) applies. The UK International Data Transfer Addendum applies to UK transfers, and the SCCs are deemed amended as required by Swiss law for transfers subject to the FADP. Where an alternative valid transfer mechanism (such as an adequacy decision or approved data transfer framework) is available, the parties may rely on that mechanism in lieu of the SCCs.

8. Data Subject requests

Taking into account the nature of the Processing, PestMetry will provide reasonable assistance, by appropriate technical and organizational measures and insofar as this is possible, to enable Customer to respond to requests from Data Subjects to exercise their rights under Data Protection Laws, including rights of access, rectification, erasure, restriction, portability, and objection. If PestMetry receives a request from a Data Subject relating to Personal Data Processed on behalf of Customer, PestMetry will not respond directly (other than to acknowledge receipt or to direct the individual to Customer) and will forward the request to Customer without undue delay.

9. Personal Data breach notification

PestMetry will notify Customer without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Personal Data Breach affecting Customer's Personal Data. The notification will, to the extent then known, describe the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, and the measures taken or proposed to address the breach and mitigate its possible adverse effects. PestMetry will cooperate reasonably with Customer's investigation and reporting obligations. PestMetry's notification of, or response to, a Personal Data Breach under this Section is not an acknowledgment by PestMetry of any fault or liability.

10. Data Protection Impact Assessments and prior consultation

Taking into account the nature of the Processing and the information available to PestMetry, PestMetry will provide reasonable assistance to Customer with any data protection impact assessments and prior consultations with Supervisory Authorities that Customer is required to carry out under Data Protection Laws in relation to the Services.

11. Audit and information rights

PestMetry will make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and will allow for and contribute to audits, including inspections, conducted by Customer or an independent auditor mandated by Customer (subject to reasonable confidentiality obligations). PestMetry may satisfy audit obligations by providing (a) written responses to reasonable information requests, and (b) then-current third-party certifications, audit reports, or attestations relevant to the Services. On-site audits, if required by Data Protection Laws, will be conducted no more than once per twelve (12) month period (except following a confirmed Personal Data Breach or where required by a Supervisory Authority), on reasonable prior written notice, during regular business hours, and in a manner that does not unreasonably interfere with PestMetry's operations or compromise the confidentiality of other customers' data.

12. Return and deletion of Personal Data

Upon expiration or termination of the Agreement, or earlier upon Customer's written request, PestMetry will, at Customer's election, return to Customer or delete Personal Data Processed on behalf of Customer, except to the extent PestMetry is required by applicable law to retain some or all of the Personal Data. Where retention is required, PestMetry will continue to protect that Personal Data in accordance with this DPA and will Process it only for the purpose and duration required by such law. Customer acknowledges that Personal Data may persist in routine backups for a limited period consistent with PestMetry's backup retention schedule, after which it will be deleted or overwritten in the ordinary course.

13. Liability

Each party's liability arising out of or related to this DPA, whether in contract, tort, or under any other theory of liability, is subject to the exclusions and limitations of liability set forth in the Agreement. Any claims brought under this DPA will be subject to the terms and conditions, including the aggregate liability caps, in the Agreement.

14. Governing law and jurisdiction

This DPA is governed by, and will be construed in accordance with, the governing law and jurisdiction provisions of the Agreement, unless otherwise required by Data Protection Laws. Where the SCCs apply, the choice of governing law and forum in the SCCs will prevail with respect to the subject matter of the SCCs.

15. Order of precedence

If there is any conflict between this DPA and the Agreement, this DPA will prevail with respect to Processing of Personal Data. If there is any conflict between this DPA and the SCCs, the SCCs will prevail with respect to the subject matter of the SCCs.

16. Changes to this DPA

We may update this DPA from time to time to reflect changes in Data Protection Laws, our Services, or industry practice. If we make material changes, we will provide reasonable notice, for example by email or an in-product notification. Continued use of the Services after the effective date of the updated DPA constitutes acceptance of the changes, except where a signed order form or master agreement expressly provides otherwise.

Annex I — Details of Processing

Subject matter: Provision of the PestMetry warehouse pest management and sanitation intelligence platform and related services.

Duration: For the term of the Agreement, plus any period during which PestMetry is required to retain Personal Data by law or to complete return or deletion obligations under Section 12.

Nature and purpose: Hosting, storing, organizing, analyzing, transmitting, and displaying Personal Data to enable Customer and its Authorized Users to record pest incidents, manage sanitation and work orders, perform inspections, digitize and interact with facility blueprints, generate reports, and administer their organization on the platform.

Categories of Data Subjects: Customer's Authorized Users (e.g., pest control managers, sanitation managers, food safety professionals, operations personnel, administrators), third-party service providers and contractors that Customer invites to the platform, and any individuals whose Personal Data Customer chooses to submit to the Services.

Categories of Personal Data: Contact and account information (name, business email, phone number, job title, employer), authentication data (hashed passwords, session tokens, SSO identifiers), user activity and audit logs, device and technical information (IP address, browser and device identifiers), photographs and images uploaded in connection with incidents, inspections, or blueprints, geolocation associated with facility records, and any additional Personal Data Customer submits.

Sensitive data: PestMetry does not require and does not intend to Process special categories of data. Customer agrees not to submit special categories of data except as expressly permitted in writing.

Frequency: Continuous, for the duration of the Agreement.

Retention: Personal Data is retained for the duration of the Agreement and as described in Section 12 and PestMetry's Privacy Policy.

Competent Supervisory Authority (for EEA/UK transfers): The Supervisory Authority of the EEA member state in which the data exporter is established, or where the data exporter is not established in the EEA, the Supervisory Authority selected in accordance with Clause 13 of the SCCs. For UK transfers, the UK Information Commissioner's Office.

Annex II — Technical and Organizational Measures

PestMetry maintains a written information security program that includes the following measures, which may be updated over time provided the overall level of security is not materially diminished:

- **Encryption:** TLS 1.2+ for data in transit; AES-256 (or equivalent) encryption for data at rest.
- **Access controls:** Role-based access control, least-privilege administrative access, mandatory multi-factor authentication for privileged accounts, and periodic access reviews.
- **Network security:** Segregated production environments, firewalls, private networking for data stores, and monitoring for anomalous activity.
- **Application security:** Secure software development lifecycle, code review, dependency scanning, and periodic vulnerability testing.
- **Logging and monitoring:** Centralized logging of security-relevant events, alerting on suspicious activity, and audit trails for administrative actions.

- **Data segregation:** Logical multi-tenant separation with row-level security enforcing tenant boundaries.
- **Personnel security:** Background checks where permitted by law, confidentiality obligations, and role-appropriate security and privacy training.
- **Business continuity:** Regular backups, documented disaster recovery procedures, and periodic restoration testing.
- **Incident response:** Documented incident response plan, defined severity levels, and customer notification workflows.
- **Vendor management:** Security and privacy reviews of Sub-processors before onboarding and on a recurring basis.

Contact

Questions about this DPA, or requests to execute a countersigned copy, can be sent to support@pestmetry.com. For a signed version, please include your legal entity name, jurisdiction of incorporation, and the name and title of your authorized signatory.