Data Processing Agreement (DPA)

Effective Date: 1 August 2025

Aikido Security BV

This Data Processing Agreement, including all schedules attached hereto, (the "DPA") is incorporated into and forms part of the Terms of Service OR the Aikido Security Master Subscription Agreement (MSA), as applicable (the "Agreement") entered into by and between Customer and Aikido. All capitalized terms used, but not defined in this DPA shall have the meanings set forth in the Agreement. In the event of a conflict between the Agreement and the DPA, the terms of the DPA shall prevail.

1. Definitions

Data Protection Laws	All national, federal, state, provincial, or local privacy, cybersecurity, and data protection laws, together with any implementing or supplemental rules and regulations, applicable to Aikido's processing of Personal Data as necessary to provide the Services as further described in the Agreement. Such Data Protection Laws shall include, without limitation: The California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations ("CCPA"), The General Data Protection Regulation means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR") or the "UK GDPR" which means the UK General Data Protection Regulation, as it forms part of the law of the UK by virtue of section 3 of the European Union (Withdrawal) Act 2018.
EU SCCs	The standard contractual clauses attached to the European Commission's Implementing Decision (EU) 2021/914 are found at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.
Personal Data	Any information relating to an identified or identifiable natural person, which is processed by Aikido, as part of the Services under the Agreement.
Restricted Transfer	Any transfer of Personal Data would be restricted by the Data Protection Laws in the absence of the EU SCCs or UK SCCs, as applicable, including appropriate addenda.
Technical and Operational Measures	The measures taken by Aikido in reference to Article 32 of the GDPR, as further detailed in Schedule 2 of this DPA.

UK Addendum	the International Data Transfer Addendum to EU SCCs, issued by the ICO under s119A(1) of the Data Protection Act 2018, version B1.0, and any updates or replacements as may be issued by the ICO from time to time in accordance with S119A(1).
UK SCCs	the UK Addendum, as amended or replaced from time to time, pursuant to Article 46 of the UK GDPR.

The terms "controller", "processor", "data subject", "process" and "supervisory authority," and their derivatives and analogous terms shall have the same meaning as set out in applicable Data Protection Laws.

2. RIGHTS AND OBLIGATIONS

2.1 **Purpose.** For the purposes of this DPA, Customer acts as the Data Controller and Aikido acts as the Data Processor with respect to the Personal Data processed under the Agreement. The processing of Personal Data happens only on instruction from the Customer and not for any other purpose. It shall only last for the duration of the use by Customer of the Products and Services as set out in the Agreement, after which the Personal Data will be deleted in accordance with the process set out in the Agreement.

2.2 **Processing instructions.** The parties agree that the Agreement and this DPA shall constitute the Customer's instructions for the processing of Personal Data. Each Party shall comply with its respective obligations under the Data Protection Laws. Aikido shall assist Customer in complying with Customer's obligations under the Data Protection Laws. Aikido's security commitments and Security Incident obligations with respect to Personal Data are specified in the Agreement. Additionally, the process for deleting Customer Data, including Personal Data, as outlined in the Agreement

2.3 **Audit.** As required by the Data Protection Law, Aikido shall keep a written record of its processing activities with respect to Personal Data. Upon reasonable prior notice, Aikido shall make available to Customer all information necessary to demonstrate compliance with this DPA. Additionally, Aikido will allow and contribute to audits (including on-site inspections) by Customer or an independent auditor mandated by Customer, to verify Aikido's compliance with its obligations under this DPA. Such audits shall be at Customers expense, subject to appropriate confidentiality, conducted no more than once annually (unless a Data Breach or suspected material non-compliance has occurred), and carried out in a manner that minimizes disruption to Aikido's business. In lieu of or prior to an on-site audit, Aikido may first provide current ISO 27001 certificates, SOC 2 attestation reports, summary audit reports, or other relevant documentation to address the information requests. Customer agrees to review these materials in good faith before requesting any further audit.

2.4 **Security.** Aikido will establish and maintain appropriate administrative, technical, and physical safeguards and controls (Technical and Operational Measures) to: (i) ensure the ongoing confidentiality, integrity, availability, and resilience of the Products and Services and Customer Content; (ii) restore the availability and access to Customers Content in a timely manner in the

event of a physical or technical incident; and (iii) have in place the process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing through the Products and Services.

2.5 **Confidentiality.** Personal Data received by Aikido under the scope of this DPA will only be used for the purposes of the Agreement and Aikido will not reproduce, disseminate, or disclose this Personal Data to any person, except to its employees and authorized representatives (e.g. temporary employees, consultants, and contractors) who need to know for the purposes of the Agreement and are bound by confidentiality obligations at least as restrictive as those in this section. Aikido will treat the received Personal Data with the same degree of care as it treats its own information of similar sensitivity, but never with less than reasonable care. The obligations in this section survive for three (3) years following expiration or termination of the Agreement. Any receive Personal Data retained in backup media will continue to be subject to this section until it is deleted.

2.6 **Permitted Disclosure.** Aikido may disclose received Personal Data (i) as approved in writing and signed by Customer; (ii) as necessary to comply with any law or valid order of a court or other governmental body; or (iii) as necessary to establish the rights of Aikido, but in the case of (ii) and (iii), only if Aikido promptly notifies Customer of the details of the required disclosure and gives Customer all assistance reasonably required to enable Aikido to take available steps to prevent the disclosure or to ensure that disclosure occurs subject to an appropriate obligation of confidence.

2.7 **Liability.** Aikido's liability under this DPA shall be subject to the limitations and exclusions of liability set forth in the Agreement. Nothing in this DPA shall increase or expand Aikido's liability beyond what is provided in the Agreement.

3. SUBPROCESSORS

3.1 Customer grants Aikido general authorization to engage third parties to process the Personal Data ("Sub-processors"). Aikido shall maintain an up-to-date list of Subprocessors at https://trustcenter.aikido.dev/subprocessors.

3.2 Aikido shall provide Customer with at least 14 days' prior written notice of its intent to add or replace a Sub-Processor. If Customer does not object in writing to the proposed change within 14 days of receipt of such notice, Customer shall be deemed to have consented to the change. If Customer objects to the proposed change within the 14-day period and Aikido does not agree with the objection, Customer shall be entitled to terminate the Agreement by providing written notice to Aikido.

3.3 Aikido shall ensure each Sub-processor is appointed pursuant to a written contract conferring materially the same obligations with respect to Personal Data as this DPA and shall be responsible for ensuring each such Sub-processor complies with all such obligations.

4. DATA REQUESTS

4.1 Aikido shall, taking into account the nature of the processing, provide reasonable assistance to Customers responding to requests from data subjects under the Data Protection Laws.

4.2 In the event Aikido becomes subject to a request from a public authority to disclose any Personal Data, Aikido shall review the legality of such a request prior to acceding to it. To the extent permitted by law, Aikido shall promptly notify Customer in writing of any such request. Aikido shall comply with such requests only in the event and to the extent that it is lawfully compelled to do so. Aikido shall in respect of any such request only disclose the minimum amount of Personal Data required.

5. GDPR

5.1 This Section shall apply only to the extent that Personal Data contains personal information subject to the GDPR or the UK GDPR and shall apply in addition to the other requirements of the Agreement and the other provisions of this DPA. The parties agree that Aikido may process Personal Data as part of providing the Services pursuant to the Agreement. Aikido shall inform Customer if it becomes aware that Customer’s instructions infringe GDPR or UK GDPR (as applicable) but without obligation to actively monitor Customer's compliance therewith.

6. INTERNATIONAL DATA TRANSFERS

6.1 Customer acknowledges and agrees that Aikido may transfer, access, and process Personal Data on a global basis as necessary to provide the Services in accordance with the Agreement. Aikido will make any such transfers in compliance with the Data Protection Laws.

6.2 The parties agree that the terms of the EU SCCs Module Two (Controller to Processor) apply to any Restricted Transfer under GDPR from Customer (as data exporter) to Aikido (as data importer).

6.3 The parties agree that the terms of the UK SCCs apply to any Restricted Transfer under the UK GDPR from Customer (as data exporter) to Aikido (as data importer).

6.4 To the extent that Aikido makes an onward transfer which is a Restricted Transfer, it shall take such measures as may be necessary to ensure that the transfer is made in compliance with the Data Protection Laws.

6.5 For the purposes of the EU SCCs: the chosen Member State for Clause 17 (governing law) shall be Belgium (unless EU Data Protection Law requires it to be the country of Customer’s establishment), and the supervisory authority of Belgium (the Belgian Data Protection Authority) shall act as the competent authority unless the SCCs require otherwise. Schedule 1 of this DPA shall be deemed Annex I of the EU SCCs (Modules 2 and 3, as applicable) and the UK Addendum, and Schedule 2 of this DPA shall be deemed Annex II (Technical and Organisational Measures) of the EU SCCs.

7. CCPA

7.1 This Section shall apply only to the extent that Personal Data contains personal information subject to the CCPA and shall apply in addition to the other requirements of the Agreement and the other provisions of this DPA.

7.2 Customer may, upon providing Aikido prior written notice, take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data by Aikido.

7.3 Aikido processes the Personal Data subject to CCPA for or on behalf of Customer for the business purposes specified in the Agreement. Aikido shall not retain, use or disclose Personal Data for any purposes other than pursuant to the business relationship of the parties and performing the Services under the Agreement or as otherwise permitted by Service Providers by the CCPA.

7.4 Aikido shall not sell Personal Data within the meaning of the CCPA. To the extent the CCPA is applicable, the parties acknowledge that Customer's transfer of Personal Data to Processor is not a "sale" and Processor provides no monetary or other valuable consideration to Controller in exchange for the Personal Data.

7.5 To the extent any Personal Data hereunder is deidentified by Aikido or Customer, Aikido shall take reasonable measures to ensure the deidentified Personal Data cannot be associated with a consumer or household and shall not attempt to reidentify such deidentified Personal Data.

7.6 Aikido certifies that it understands the obligations and restrictions contained in this Section 7 and will comply with them.

8. GENERAL

8.1 Governing Law. Unless otherwise required, the parties agree that:
The Agreement is governed by and construed under the laws of Belgium, without regard to any conflict of law rules or principles, and excluding the application of the United Nations Convention on Contracts for the International Sale of Goods. The Parties irrevocably submit to the exclusive jurisdiction of the courts of competent jurisdiction in Ghent, Belgium (for Agreements with Aikido Security BV). Parties will first try to settle any dispute between them amicably in good-faith negotiations prior to seeking enforcement from a court.

8.2 Updates. Aikido may modify this DPA as required as a result of (a) changes in Data Protection Laws; (b) a merger, acquisition, corporate reorganization, or other similar occurrences; or (c) the release of new features, functions, products or services or material changes to any of the existing Services. Aikido may make such modifications by posting a revised version of this DPA at https://www.aikido.dev/ or by otherwise notifying the Customer. The modified version of the DPA will become effective upon posting. By continuing to use the Services after the effective date of any modifications to this DPA, the Customer agrees to be bound by the modified DPA.

SCHEDULE 1: DATA PROCESSING DETAILS

Categories of data subjects	Developers and other employees of Customer who are users of Aikido's services or otherwise contribute to Customer's code base.
Categories of personal data	First and last name, employer, title, and position Email Addresses User ID on source code repositories and other services integrated with Aikido by the Customer's users Connection and/or localization data
Sensitive data transferred (if applicable)	None.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	Ongoing.
Nature of the processing	The processing of certain personal data by the Processor on behalf of the Controller in relation to allowing access of the Controller's users to the Processor's platform for the purposes of reviewing software projects submitted to the platform.
Purpose(s) of the data transfer	Providing the Services pursuant to the Agreement
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	As set forth in the Agreement
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	See https://trustcenter.aikido.dev/subprocessors for details.

SCHEDULE 2: TECHNICAL AND OPERATIONAL MEASURES TO PROTECT THE PERSONAL DATA

Aikido may update or modify its Technical and Organizational Measures from time to time, provided such updates do not result in a material reduction of the protection provided for Personal Data.

Accountability and Certification

Aikido Security BV follows internal governance protocols to ensure compliance with data protection regulations.

External certifications, such as ISO/IEC 27001 and SOC2, are maintained to demonstrate compliance with security standards.

What follows are a selection of relevant policies describing technical and organisational measures undertaken.

Infrastructure security

Unique production database authentication enforced

The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key.

Encryption key access restricted

The company restricts privileged access to encryption keys to authorized users with a business need.

Access control procedures established

The company's access control policy documents the requirements for the following access control functions:

* adding new users;

* modifying users; and/or

* removing an existing user's access.

Production database access restricted

The company restricts privileged access to databases to authorized users with a business need.

Firewall access restricted

The company restricts privileged access to the firewall to authorized users with a business need

Production OS access restricted

The company restricts privileged access to the operating system to authorized users with a business need

Production network access restricted

The company restricts privileged access to the production network to authorized users with a business need

Access revoked upon termination

The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs

Unique network system authentication enforced

The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys

Remote access MFA enforced

The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method

Remote access encrypted enforced

The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.

Intrusion detection system utilized

The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.

Log management utilized

The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives

Network segmentation implemented

The company’s network is segmented to prevent unauthorized access to customer data

Network firewalls reviewed

The company reviews its firewall rulesets at least annually. Required changes are tracked to completion,

Network firewalls utilized

The company uses firewalls and configures them to prevent unauthorized access.

Network and system hardening standards maintained

The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.

Organizational security

Asset disposal procedures utilized

The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.

Portable media encrypted

The company encrypts portable and removable media devices when used

Anti-malware technology utilized

The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.

Employee background checks performed

The company performs background checks on new employees

Code of Conduct acknowledged by contractors

The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.

Code of Conduct acknowledged by employees and enforced

The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.

Confidentiality Agreement acknowledged by contractors

The company requires contractors to sign a confidentiality agreement at the time of engagement.

Confidentiality Agreement acknowledged by employees

The company requires employees to sign a confidentiality agreement during onboarding.

Performance evaluations conducted

The company managers are required to complete performance evaluations for direct reports at least annually.

Password policy enforced

The company requires passwords for in-scope system components to be configured according to the company's policy.

MDM system utilized

The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.

Visitor procedures enforced

The company requires visitors to sign-in, wear a visitor badge, and be escorted by an authorized employee when accessing the data center or secure areas.

Product security

Data encryption utilized

The company's datastores housing sensitive customer data are encrypted at rest.

Control self-assessments conducted

The company performs control self-assessment at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA

Penetration testing performed

The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs

Data transmission encrypted

The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.

Vulnerability and system monitoring procedures established

The company's formal policies outline the requirements for the following functions related to IT / Engineering:

* vulnerability management;

* system monitoring.

Internal security procedures

Continuity and Disaster Recovery plans established

The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel

Continuity and disaster recovery plans tested

The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.

Cybersecurity insurance maintained

The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions

Configuration management system established

The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.

Development lifecycle established

The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements

Whistleblower policy established

The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns

Board oversight briefings conducted

The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed

Board charter documented

The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.

Board expertise developed

The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed

Board meetings conducted

The company's board of directors meets at least annually and maintains formal meeting minutes, The board includes directors that are independent of the company,

Backup processes established

The company's data backup policy documents requirements for backup and recovery of customer data

System changes externally communicated

The company notifies customers of critical system changes that may affect their processing,

Management roles and responsibilities defined

The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.

Organization structure documented

The company maintains an organizational chart that describes the organizational structure and reporting lines, Roles and responsibilities specified

Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

Security policies established and reviewed

The company’s information security policies and procedures are documented and reviewed at least annually.

Support system available

The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.

System changes communicated

The company communicates system changes to authorized internal users

Access reviews conducted

The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.

Access requests required

The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned

Incident response plan tested

The company tests their incident response plan at least annually.

Incident response policies established

The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.

Physical access processes established

The company has processes in place for granting, changing, and terminating physical access to company data centers based on an authorization from control owners.

Data center access reviewed

The company reviews access to the data centers at least annually

Company commitments externally communicated

The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS)

External support resources available

The company provides guidelines and technical support resources relating to system operations to customers

Service description communicated

The company provides a description of its products and services to internal and external users.

Risk assessment objectives specified

The company specifies its objectives to enable the identification and assessment of risk related to the objectives.

Risks assessments performed

The company’s risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed, The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.

Risk management program established

The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

Third-party agreements established

The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.

Vendor management program established

The company has a vendor management program in place. Components of this program include:

* critical third-party vendor inventory;

* vendor's security and privacy requirements; and

+ review of critical third-party vendors at least annually.

Data and privacy

Data retention procedures established

The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.

Customer data deleted upon leaving

The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.

Data classification policy established

The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.