

DATA PROCESSING AGREEMENT

Orbiscend OÜ — Aevon Timesheets (Atlassian Marketplace app)
GDPR Article 28 Processor Terms — Version 1.0

Parties and Background

This Data Processing Agreement ("DPA") is entered into between:

(1) Orbiscend OÜ, a private limited company registered in Estonia, with its registered office at Ahtri 12, Tallinn 15551, Estonia (the "Processor", "we", "us", or "Orbiscend"; the same party identified as the "Provider" under the Principal Agreement); and

(2) the customer organisation that installs, subscribes to, or uses the App, as identified in the Principal Agreement (the "Controller", "you", or "Customer"),

each a "Party" and together the "Parties".

Background. The Customer uses Aevon Timesheets, an Atlassian Forge app published by Orbiscend on the Atlassian Marketplace (the "App"), within the Customer's Atlassian Cloud (Jira) environment. In providing the App, Orbiscend processes Personal Data on the Customer's behalf. This DPA governs that processing and forms part of, and is subject to, the agreement under which the Customer is licensed to use the App (the "Principal Agreement") — namely the Atlassian Marketplace standard end-user agreement (the Bonterms Standard End User Agreement) together with Orbiscend's Provider-Specific Terms. This DPA is the "Data Protection Addendum" identified in those Provider-Specific Terms for the purposes of the Principal Agreement. If there is a conflict between this DPA and the Principal Agreement on the subject of data protection, this DPA prevails.

Effective date. This DPA is effective from the date on which the Customer first installs, enables, or uses the App, or otherwise accepts the Principal Agreement.

1. Definitions

Capitalised terms not defined here have the meaning given in the GDPR. "GDPR" means Regulation (EU) 2016/679 and, where applicable, the UK GDPR and the Data Protection Act 2018. "Applicable Data Protection Law" means all privacy and data protection laws applicable to the processing under this DPA, including the GDPR and, where applicable, the California Consumer Privacy Act as amended ("CCPA/CPRA"). "Personal Data", "processing", "data subject", "controller", "processor" and "personal data breach" have the meanings given in the GDPR. "Sub-processor" means any third party engaged by the Processor to process Personal Data on the Customer's behalf. "End-User Data" means the Personal Data described in Annex 1 that is processed in connection with the App.

2. Roles and Scope of Processing

2.1 For Personal Data processed in connection with the App, the Customer acts as the controller (or as a processor acting on behalf of its own controllers) and Orbiscend acts as the processor. For the purposes of the CCPA/CPRA, Orbiscend acts as a "service provider" and processes Personal Data solely on the Customer's behalf and for the business purposes set out in Annex 1.

2.2 Orbiscend processes End-User Data only for the purpose of providing, maintaining, securing and supporting the App, and only on the Customer's documented instructions, which are given through: (a) this DPA and the Principal Agreement; (b) the Customer's configuration and use of the App; and (c) any further written instructions agreed by the Parties.

- 2.3 Orbiscend does not sell or share End-User Data (as those terms are defined under the CCPA/CPRA) and does not retain, use or disclose End-User Data for any purpose other than performing the App services, or as otherwise permitted by Applicable Data Protection Law. Orbiscend will not combine End-User Data with personal information from other sources except as permitted by the CCPA/CPRA.
- 2.4 The subject matter, duration, nature and purpose of the processing, the types of Personal Data and the categories of data subjects are set out in Annex 1.
- 2.5 If Orbiscend is required by EU or Member State law to process End-User Data other than on the Customer's instructions, it will inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3. Orbiscend's Obligations

Orbiscend will:

- 3.1 Instructions. process End-User Data only on the Customer's documented instructions as described in clause 2, including with regard to international transfers, and promptly inform the Customer if, in its opinion, an instruction infringes Applicable Data Protection Law;
- 3.2 Confidentiality. ensure that the co-founders and any other personnel authorised to process End-User Data are bound by an appropriate duty of confidentiality and process End-User Data only as necessary to provide and support the App;
- 3.3 Security. implement and maintain the technical and organisational measures set out in Annex 2 to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR;
- 3.4 Sub-processing. respect the conditions in clause 5 for engaging Sub-processors;
- 3.5 Data-subject rights. taking into account the nature of the processing, assist the Customer by appropriate technical and organisational measures, insofar as possible, to respond to requests to exercise data-subject rights under Chapter III GDPR, as further described in clause 9;
- 3.6 Assistance. assist the Customer in ensuring compliance with its obligations under Articles 32 to 36 GDPR (security of processing, breach notification, data protection impact assessments and prior consultation), taking into account the nature of processing and the information available to Orbiscend;
- 3.7 Deletion or return. at the Customer's choice, delete or return all End-User Data after the end of the provision of services relating to processing, and delete existing copies unless retention is required by law, as further described in clause 11; and
- 3.8 Audits and information. make available to the Customer all information necessary to demonstrate compliance with the obligations in Article 28 GDPR and allow for and contribute to audits, as described in clause 10.

4. Customer's Obligations

- 4.1 The Customer warrants that it has a lawful basis for the processing of End-User Data and for the instructions it gives, that it has provided all required notices and obtained any required consents from data subjects, and that its instructions comply with Applicable Data Protection Law.
- 4.2 The Customer is responsible for the security and lawful administration of its own Atlassian environment and user accounts, including the configuration of permissions, roles and data-residency settings made available by Atlassian.

5. Sub-processing

- 5.1 The Customer grants Orbiscend a general authorisation to engage the Sub-processors listed in Annex 3. Aevon Timesheets is a Forge-native app: End-User Data is stored and processed within the Atlassian Forge platform and native Jira, and the only Sub-processor of End-User Data is Atlassian, which provides the underlying platform, hosting and storage. Orbiscend's other business providers (for example, its website host, business-email provider and development-tooling providers) do not receive End-User Data.
- 5.2 Orbiscend will impose on each Sub-processor, by contract, data-protection obligations that are no less protective than those in this DPA, in particular providing sufficient guarantees to implement appropriate technical and organisational measures. Orbiscend remains fully liable to the Customer for the performance of each Sub-processor's obligations.
- 5.3 Orbiscend will give the Customer prior written notice (which may be by email or by updating the list in Annex 3 or a referenced webpage) of any intended addition or replacement of a Sub-processor, giving the Customer a reasonable opportunity to object on reasonable data-protection grounds. If the Parties cannot resolve a timely objection, the Customer may, as its sole remedy, terminate the App subscription in respect of the affected processing.

6. International Data Transfers

- 6.1 End-User Data is hosted within the Atlassian platform, and its storage location is determined by Atlassian's infrastructure and any data-residency options the Customer has configured. Orbiscend does not transfer End-User Data to any separate storage of its own.
- 6.2 To the extent any processing involves a transfer of Personal Data outside the EEA, the UK or another jurisdiction requiring a transfer mechanism, the Parties agree that the European Commission's Standard Contractual Clauses (Module Two: controller-to-processor), and the UK International Data Transfer Addendum where applicable, are incorporated into this DPA by reference and completed using the details in the Annexes, with Orbiscend as "data importer" and the Customer as "data exporter". As Orbiscend is established in the European Economic Area (Estonia), these clauses apply only to the extent the processing actually involves a restricted transfer; platform-level transfers within Atlassian are governed by Atlassian's own transfer mechanisms.

7. Security Measures

- 7.1 Orbiscend implements and maintains the technical and organisational measures described in Annex 2. The Customer acknowledges that core platform security controls (including encryption, infrastructure security, availability and backups) are provided by Atlassian under Atlassian's certifications, and that Orbiscend inherits and relies on those controls under the Forge shared-responsibility model.
- 7.2 Orbiscend may update its security measures from time to time provided that the updates do not materially reduce the overall level of security.

8. Personal Data Breach

- 8.1 Orbiscend will notify the Customer without undue delay, and in any event within 72 hours, after becoming aware of a personal data breach affecting End-User Data.
- 8.2 The notification will describe, to the extent known and as it becomes available: 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 it and mitigate its effects. Orbiscend

will reasonably cooperate with the Customer and take reasonable steps to mitigate and remediate the breach.

9. Data-Subject Requests and Assistance

- 9.1 If Orbiscend receives a request from a data subject in respect of End-User Data, it will, unless legally required to respond, promptly forward the request to the Customer and will not respond directly except on the Customer's documented instructions.
- 9.2 Taking into account the nature of the processing, Orbiscend will provide reasonable assistance, including by appropriate technical and organisational measures, to enable the Customer to respond to requests to exercise data-subject rights (access, rectification, erasure, restriction, portability and objection). Because End-User Data resides within the Customer's Atlassian environment, much of this data is directly accessible to, and manageable by, the Customer through Atlassian and the App.

10. Audits and Demonstration of Compliance

- 10.1 Orbiscend will make available to the Customer, on reasonable written request, the information reasonably necessary to demonstrate compliance with this DPA and Article 28 GDPR, including its security documentation, its CAIQ self-assessment for the App, and evidence of Atlassian's certifications on which it relies.
- 10.2 Where the Customer reasonably requires further information to satisfy an audit obligation under Applicable Data Protection Law, the Parties will agree in advance the scope, timing and reasonable cost of such an audit, conducted no more than once per year (except where required by a supervisory authority or following a personal data breach), on reasonable notice, during business hours, and subject to confidentiality, so as not to disrupt Orbiscend's operations.

11. Return and Deletion of End-User Data

- 11.1 End-User Data managed by the App is stored within Atlassian Forge storage and native Jira. On expiry or termination of the App subscription, or on uninstallation of the App, App-managed data follows Atlassian's Forge data lifecycle and is deleted accordingly. Personal Data held in native Jira (for example, worklogs) remains under the Customer's control in its Atlassian environment.
- 11.2 Orbiscend keeps no separate copy of End-User Data outside the Atlassian platform. On the Customer's written request made before deletion, Orbiscend will, where technically feasible, assist the Customer in exporting App-managed data prior to deletion. Orbiscend may retain Personal Data to the extent required by law, in which case it will continue to protect it under this DPA.

12. Liability

Each Party's liability arising out of or related to this DPA is subject to the limitations and exclusions of liability set out in the Principal Agreement, including the liability caps in section 14 of the Standard End User Agreement. The Parties acknowledge that claims arising from a breach of this DPA or of data-protection or security obligations are treated as "Enhanced Claims" under the Principal Agreement and are subject to the Enhanced Cap (three times the General Cap), save for liabilities that cannot be limited under applicable law.

13. Term and Termination

This DPA takes effect on the Effective Date and remains in force for as long as Orbiscend processes End-User Data on the Customer's behalf under the Principal Agreement. Provisions that by their nature should survive termination (including confidentiality, deletion and liability) survive.

14. Governing Law and Miscellaneous

- 14.1 This DPA is governed by the same law as the Principal Agreement — under the Atlassian Marketplace standard agreement's default, the laws of the State of California (with the courts of San Francisco, California), unless the Parties specify otherwise in the Provider-Specific Terms — without prejudice to any mandatory provisions of Applicable Data Protection Law. Where the Standard Contractual Clauses apply under clause 6, those clauses are instead governed by the law their own terms require (the law of an EU member state that allows third-party-beneficiary rights).
- 14.2 If any provision of this DPA is held invalid or unenforceable, the remaining provisions continue in full force, and the Parties will replace the invalid provision with a valid one that achieves its purpose as closely as possible.
- 14.3 This DPA, together with the Principal Agreement and its Annexes, is the entire agreement between the Parties on the subject of processing of End-User Data and supersedes any prior data-processing terms on that subject.

15. Acceptance

This DPA is incorporated into the Principal Agreement and is accepted by the Customer when the Customer installs, enables, or uses the App, or otherwise accepts the Principal Agreement. The Parties are not required to sign this DPA separately for it to be binding. On request, Orbiscend will provide a copy of this DPA executed by Orbiscend for counter-signature by the Customer; such requests may be sent to legal@orbiscend.com.

Annex 1 — Description of the Processing

- Controller: the Customer — the Atlassian customer organisation that installs, subscribes to, or uses the App.
- Processor: Orbiscend OÜ, Ahtri 12, Tallinn 15551, Estonia.
- App: Aevon Timesheets — an Atlassian Forge app providing time tracking, timesheet submission and approval, and billing review within the Customer's Jira environment.
- Subject matter: processing of Personal Data within the Customer's Atlassian (Jira) environment as necessary to provide and support the App.
- Duration: for the term of the App subscription or installation; data follows the Atlassian Forge data lifecycle on uninstall (see clause 11).
- Nature and purpose: recording and displaying worked time; routing and recording timesheet approvals; producing reports and cross-team billing review; and sending in-product and Jira notifications related to these functions.
- Processing location: within the Atlassian Forge platform and native Jira; storage location determined by Atlassian and the Customer's data-residency configuration. No separate storage by Orbiscend.

Categories of data subjects

- The Customer's personnel — employees, contractors and other users — who log time in, or are referenced by, the App (for example as worklog authors, approvers, reviewers, or account owners).

Types of Personal Data

- Account identifiers and profile data: Atlassian account IDs, and — as exposed by Jira's user API and permission model — display names, avatar URLs and email addresses. Account IDs are stored as references within the App's records; display name, avatar and email are read transiently for in-product

display and are not stored by the App. Notifications are routed by account ID through Jira's native notification service.

- Time-tracking records: worklogs authored by users — date, duration, the associated Jira issue or project, and optional free-text descriptions or comments (stored natively in Jira).
- Worklog and timesheet metadata: billable flags and admin-defined custom attributes attached to worklogs; account and category billing assignments; timesheet approval-workflow records (submitted periods, approver assignments, approval/rejection/recall events and timestamps); and permission and approver-routing configuration referencing users by account ID, group or project role (stored in Forge storage).
- Special categories of data: none. The App is not intended to process special-category (Article 9) Personal Data. Personal Data processed is minimal — primarily Atlassian account IDs, with display name and (transiently) email address as provided by Jira.

Annex 2 — Technical and Organisational Measures

Orbiscend implements the following measures, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing, as well as the risks to data subjects:

Platform and encryption (inherited from Atlassian)

- The App is built on Atlassian Forge and operates no servers or datacentres of Orbiscend's own. Infrastructure security, availability and backups are provided by Atlassian under its certifications (SOC 2 Type II; ISO/IEC 27001, 27017, 27018, 27701; CSA STAR Level 2).
- Encryption in transit (TLS 1.2+) and at rest (AES-256) is provided by the Forge platform. Orbiscend stores no credentials or cryptographic keys.

Data minimisation and isolation

- End-User Data remains within Atlassian (Forge storage and native Jira); Orbiscend keeps no separate copy and the App makes no egress of End-User Data to external hosts or third parties.
- The App requests only the minimum Atlassian scopes required for its functionality (least privilege).
- Only minimal Personal Data is processed (account IDs, display names, transient email addresses).

Access control

- Administrative access to production (Atlassian/Forge, source control, domain/email) is limited to Orbiscend's co-founders.
- Multi-factor authentication is enabled on all such accounts; workstations use full-disk encryption, automatic screen-lock and a password manager with unique strong credentials.
- Within the App, access to data and administrative functions is enforced server-side using Jira permissions (including the App's custom global permissions for administrator, account-administrator and reviewer roles).

Secure development and vulnerability management

- Source code is version-controlled; changes are made via reviewed pull requests before merge.
- Continuous-integration security scanning runs on every change and on a weekly schedule: dependency/SCA scanning (Dependabot, npm audit, OSV-Scanner), static analysis (SAST, Semgrep) and secret scanning (Gitleaks).
- Changes are validated in a Forge development/staging environment before production deployment; Forge supports versioned deployments and rollback.

Resilience

- Availability, redundancy, backup and disaster recovery for the platform and customer data are provided by Atlassian. The App is stateless beyond Forge storage and re-deployable from source (target RTO: 1 business day; RPO approximately 0 for App-managed data, as persistence and backup are Atlassian's responsibility).

Incident response

- Documented detect, triage, contain, remediate and review process, with customer notification of a confirmed personal data breach within 72 hours (clause 8).

Annex 3 — Approved Sub-processors

As at the Effective Date, the Sub-processor of End-User Data is:

- Atlassian Pty Ltd (and affiliates) — Forge platform, hosting and storage. Hosts the App and stores End-User Data (Forge storage and native Jira); location per Atlassian infrastructure and the Customer's data-residency configuration.

Not Sub-processors of End-User Data. Orbiscend uses certain providers for general business operations — a website host, CDN and DNS provider; a business-email provider; and AI development-tooling — which do not receive End-User Data. They are listed for transparency on Orbiscend's security page and are not Sub-processors under this DPA.

Orbiscend OÜ · legal@orbiscend.com · privacy@orbiscend.com · security@orbiscend.com