TAIGA MASTER SERVICE TERMS

Version: v1.0, effective 6 September 2026

1. THE AGREEMENT

1.1 Parties and documents

These Master Service Terms are issued by Taiga AI Oy, Business ID 3607851-2, Lapinlahdenkatu 16, 00180 Helsinki, Finland ("Taiga"). They apply between Taiga and the customer named on a signed Order Form (the "Customer"); each is a "Party". Access to the Platform is granted only under a signed Order Form.

The Agreement consists of, in this order of precedence:

1. the Order Form, including any Special Terms recorded on it;
2. Schedule D (Data Processing), as regards the processing of personal data only;
3. the DORA Add-on, where the Customer is a financial entity within the meaning of Regulation (EU) 2022/2554, and the Public Sector Rider, where the Customer is a Finnish contracting authority or other public-sector body, each only on the matters it covers — where both apply, the Rider prevails on general terms, dispute forum, payment terms, price fixity and publicity, and the DORA Add-on prevails on audit, regulator access, incident notification, subcontracting consent, register-of-information data and exit;
4. these Master Service Terms, including Schedules A to D;
5. the Aurora Rate Card and the Service Description, in the versions published on the date of the Order Form;
6. the Acceptable Use Policy published at tai.ga/en/acceptable-use.

No other terms apply. The Agreement is complete without any industry standard terms.

These terms are published online. The version published on the date of your Order Form is the one that binds you, and nothing we publish later changes a signed deal without notice and a free way out.

1.2 Versions

The versions of these terms, the Rate Card and the Service Description published at tai.ga/legal on the date of the Order Form govern for the life of that Order Form. Taiga may publish new versions. A new version applies to an existing Order Form only on thirty (30) days' written notice with the Customer's right to terminate the affected Service without charge from the date the change would take effect, or immediately where the change is required by mandatory law or is a security fix that does not materially reduce functionality or the Customer's rights. Superseded versions stay published, dated, at a stable address on tai.ga. Nothing published on tai.ga varies a signed Order Form.

1.3 Amendments

Except as clause 1.2 provides, the Agreement is amended only in writing signed by both Parties. A step-up under clause 4.4 is a pricing mechanic within the Agreement, not an amendment of it.

2. DEFINITIONS

Capitalised words mean what this section says. Aurora and Product are the two that decide the invoice.

"Account" means the Customer organisation named on the Order Form, comprising the legal entities listed there. The Customer's own customers and end users are never part of the Account and never carry a fee.

"Account Cap" means the most the Account may consume in a calendar month: the Aurora Pool, subject to any lower ceiling the Customer's administrator sets in the Platform. The Account Cap is always on.

"Action Required" means the state the Account enters when it reaches the Account Cap and work stops. It is a normal service state, not a Taiga failure and not a Customer breach, and it is excluded from downtime under Schedule A.

"Aurora" or **"Aurora Credit"** means the unit in which consumption of the Services is measured. It has no independent monetary value, is not currency, is not transferable or refundable and confers no monetary claim. The Rate Card states what is metered, how each operation is measured and the basis on which consumption is converted into Aurora; the Aurora an operation draws follows the third-party consumption it causes, so it may differ between engines, models and types of operation and may move over time.

"Aurora Pool" means the Aurora made available to the Account for a calendar month by the Deliver + Operate step on the Order Form.

"Billing Administrator" means the person the Customer's administrator designates in the Platform to receive consumption notices and to approve or decline a step-up, and until one is designated, the administrator.

"Customer Content" means everything the Customer or its users upload to, connect to or produce through the Platform, including specifications, repositories, conversations and Delivered Software.

"Delivered Software" means the application code, infrastructure definitions, CI/CD configuration and documentation Taiga delivers to the Customer through Deliver, with the audit trail for each Build.

"Governed Run" means a run for which a named competent reviewer is recorded in the Platform audit trail before its output is promoted to production.

"Platform" means Taiga's managed EU software-as-a-service platform, the agents and models it operates, and its documentation.

"Product" means one application or one repository, which the Platform calls a project. Products are counted on the last day of each month; a change in Learn step takes effect on the first day of the following month.

"Rate Card" means the Aurora Rate Card published by Taiga, in the version published on the date of the Order Form, which states the Aurora Pool of each step, what is metered, how each operation is measured and the basis on which consumption is converted into Aurora.

"Service Description" means Taiga's published description of what the Services do, how the Platform behaves, its service levels and its support, in the version published on the date of the Order Form.

"Services" means Learn and Deliver + Operate as the Order Form records them, and **"Service"** means either.

"Taiga-hosted mode" means the hosting mode in which Taiga provides the repository and runs the runtime; **"Customer-hosted mode"** means the mode in which the Customer uses its own repositories and its own cloud account. Both run in the EU.

3. THE SERVICES

Learn is what we watch. Deliver + Operate is what we build and run. You can buy Learn alone; Deliver always sits on top of Learn.

3.1 Learn

Learn observes the Customer’s estate and produces evidence about it: the Discovery Pipeline, run for each new Product the Customer adds; a scan of every repository the Customer connects, on GitHub.com or GitHub Enterprise, for vulnerabilities, security findings and policy compliance; and rescans as the Service Description describes. Learn consumes no Aurora.

3.2 Deliver + Operate

Deliver plans, builds, tests and releases software on the Platform through the review and release checks the Service Description states, and each Build delivers code, infrastructure definitions, CI/CD configuration and its audit trail. Operate monitors Delivered Software with TaigaSense for vulnerabilities and application health, deploys it and reports delivery performance metrics. Both draw on the Aurora Pool.

Learn is mandatory whenever Deliver + Operate is on. Terminating Learn terminates Deliver + Operate; terminating Deliver + Operate leaves Learn running.

3.3 Hosting modes

The Customer chooses the hosting mode per Product in the Platform. In Customer-hosted mode Taiga reaches the Customer’s repositories only through the GitHub App the Customer installs, within the scopes it grants, holds repository content only in an isolated per-build workspace destroyed when the build ends, and deploys into the Customer’s own cloud account. In Taiga-hosted mode Taiga provides the repository and hosts the runtime in the EU.

3.4 Permitted use

The Customer may deploy, operate, distribute and commercially exploit Delivered Software, including to its own customers and end users, without restriction and without further fee. The Customer may not resell Platform access, give third parties access to the Platform or use it on behalf of unaffiliated third parties; contractors acting for the Customer in its own business may use it. Users are unlimited on every step. Use is subject to the Acceptable Use Policy.

4. FEES AND AURORA

4.1 Fees

The Learn step and the Deliver + Operate step on the Order Form each carry the monthly fee stated there, excluding value added tax. The Aurora Pool of each Deliver + Operate step, how many units of Scale may be stacked and the point above which Portfolio is the next step are those the Rate Card states. Portfolio is the ceiling.

4.2 The Aurora Pool

One Aurora Pool is made available each calendar month and both rails draw on it. Aurora unused at the end of the month expires. Aurora is never refunded, exchanged or converted.

4.3 The Account Cap

The Account Cap is always on. When the Account reaches it, the Account enters Action Required and work stops until the Customer steps up, waits for the next month or otherwise resolves the position. The Platform warns the Billing Administrator as consumption approaches the cap, on every Account.

4.4 Step-up only with your acceptance

The monthly fee rises above the steps on the Order Form only where the Customer's administrator has accepted a step-up in the Platform — in advance, up to a ceiling set there, or when the pool runs out — and only to the step accepted. A step-up never exceeds a ceiling the administrator has set, or Portfolio. The step fee is charged pro rata from the day it takes effect, the superseded fee is credited pro rata, nothing is retroactive, and the Account returns to the steps on the Order Form for the following month unless the Customer keeps the higher step. How the Platform warns, asks for acceptance and paces step-ups is described in the Service Description and may change; what does not change is that no fee rises without the Customer's acceptance.

4.5 Step-down

The Customer may step down either rail on notice, without charge, with effect from the end of the calendar month following the notice — the same period as termination — or sooner where the Platform offers it. During a committed term the steps on the Order Form are the floor.

Two rails, two lines, one invoice. The cap is always on, so the bill cannot climb without someone at your end saying yes.

4.6 The Rate Card and how Aurora is priced

The Rate Card states what is metered, how each operation is measured and the basis on which consumption is converted into Aurora. The version in force on the date of the Order Form governs. Aurora measures the third-party model-inference and runtime consumption an operation actually causes, at the prices the relevant provider charges at the time it is incurred, so the Aurora cost of an operation moves with those prices in both directions and Taiga neither fixes it nor guarantees it. Taiga may publish a new version of the Rate Card prospectively on not less than ninety (90) days' written notice stating the grounds where it changes what is metered, how an operation is measured or the conversion basis; such a version gives the Customer the right to terminate the affected Service without charge from the date it takes effect; and no change applies to work already done. A movement in a provider's own prices is not a new version and needs no notice.

4.7 What does not consume Aurora

Runs that fail because of a Platform fault, retries Taiga initiates, runs voided by a Taiga defect, agent execution beyond the published execution limit for the operation, and consumption from unauthorised use of the Customer's credentials from the earlier of Taiga detecting it and the Customer reporting it. None of these triggers a step-up or Action Required.

4.8 Metering disputes

The Customer may dispute the metering of an invoice within thirty (30) days. A disputed amount does not fall due, bears no interest and triggers no suspension. Taiga produces the run-level audit record within ten business days; where the meter was wrong, Aurora is restored, any step-up is unwound and the difference is credited. Taiga's measurement is evidence, not conclusive.

4.9 Invoicing and payment

The Learn fee and the base Deliver + Operate fee are invoiced monthly in advance on separate lines; step-up differentials in arrears. Invoices are European-standard e-invoices (Finvoice 3.0 or Peppol BIS); Taiga's e-invoicing address is OVT 003736078512, operator Maventa, 003721291126. Payment is due twenty-one (21) days net from the invoice date; for a Finnish contracting authority thirty (30) days from receipt of the invoice, as laki kaupallisten sopimusten maksuehdoista 30/2013 provides. Late-payment interest under korkolaki 633/1982 4 a § runs from the due date, and Taiga is entitled to the EUR 40 recovery compensation under perintälaki 513/1999 10 i § plus reasonable further recovery costs. Value added tax is added at the rate in force; the reverse charge applies to EU business customers outside Finland against a valid VAT number. Forbearance on interest or costs on one invoice is a waiver for that invoice only.

5. YOUR RESPONSIBILITIES

The first one matters most. A run nobody read is not a governed run, and our warranties do not follow unreviewed output into production.

5.1 Competent human review

The Customer shall ensure that a person competent to judge it reviews Platform output before it is relied on in production, and that the reviewer is recorded against the run in the audit trail, which Taiga makes available. Output promoted to production without a recorded review is accepted by the Customer as fit for its purpose. Taiga's warranties in clause 7, Schedule A and the indemnity in clause 9 do not extend to output promoted otherwise than as a Governed Run, and Taiga is not liable for defects competent review would reasonably have found. This does not apply to defects not reasonably detectable on review, to Taiga's gross negligence or wilful misconduct, or to liability that mandatory law does not allow to be limited, and it does not reduce either Party's liability toward an injured person under the law implementing Directive (EU) 2024/2853.

5.2 Information, credentials and systems

The Customer gives Taiga sufficient and correct information and instructions and is responsible for them; keeps its credentials safe and reports suspected misuse without undue delay; and maintains its own directory, repositories, cloud account and network so the Services can be provided. Taiga reaches those systems only through grants the Customer makes and may revoke.

5.3 High-risk and safety-critical use

The Customer notifies Taiga in writing before using the Platform to build a high-risk AI system within the meaning of Regulation (EU) 2024/1689, software whose defect could cause death or personal injury, a Class A system under laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä 703/2023, or anything involving security-classified material. Such use requires Taiga's written agreement and any additional review, testing and documentation Taiga specifies, charged separately. The Services are not approved for security-classified material.

6. SHARED RESPONSIBILITY

Three zones. We own the platform, you own your systems, and the software we build is reviewed, owned and, unless you buy Taiga-hosted mode, run by you.

Taiga is responsible for the Platform: its availability, patching, security, tenant isolation, agent permissions and audit trail. The Customer is responsible for its connected systems: its directory, single sign-on and user lifecycle, its repositories and cloud account, its access grants and its policies. Delivered Software is built by Taiga under the Customer's policies with the evidence produced, and is reviewed, accepted and owned by the Customer; in Customer-hosted mode the Customer runs it and is responsible for the runtime and its security, and in Taiga-hosted mode Taiga runs it. TaigaSense and Learn detect and propose; deciding to apply a fix stays with the Customer, and Taiga makes no representation that its output identifies every issue, vulnerability, defect or compliance gap.

7. WARRANTIES

We warrant the platform, the process and the delivered software at acceptance. We do not warrant that AI output is right, and we say so plainly rather than in capitals.

7.1 What Taiga warrants

Taiga warrants that the Platform conforms to the Service Description and is provided with the professional skill and care the work requires; that each Build passes through the review and release checks the Service Description states and they are recorded, that the Discovery Pipeline is produced for each new Product, and that a complete, tamper-evident audit trail is retained — with re-performance of the step as the sole remedy; and that Delivered Software conforms to the agreed specification and acceptance criteria at acceptance, with defect remediation for ninety (90) days and, failing remediation, a refund of the fees attributable to that delivery as the sole remedy. The delivery warranty does not extend to portions the Customer modifies or to defects those modifications cause.

7.2 What Taiga does not warrant

AI output is probabilistic. Taiga does not warrant that output is accurate, complete, original, free of similarity to output produced for others or reproducible; that the Services are fit for the Customer's particular purpose; that operation is uninterrupted or error-free; that Delivered Software is free of every vulnerability; or that copyright subsists in Delivered Software.

7.3 Models change

Taiga may substitute the underlying model or model provider on advance written notice. Output characteristics may change, prior acceptance does not bind Taiga to a model, and the Customer may object on documented AI-governance grounds, in which case the Parties discuss an alternative in good faith.

8. INTELLECTUAL PROPERTY

Your product is yours, from delivery, whether or not copyright turns out to exist in machine-written code. Our platform, prompts and tooling are ours.

8.1 Delivered Software is the Customer's

As between the Parties, all right, title and interest in the Delivered Software is the Customer's from delivery. Taiga assigns to the Customer all right it may have in it; to the extent any right cannot vest by assignment, Taiga grants a perpetual, irrevocable, worldwide, royalty-free, exclusive, sublicensable licence to use, modify, distribute and exploit it; and Taiga covenants not to assert any right it may hold in it. Vesting does not depend on payment; non-payment is dealt with under clause 16. This allocation is prudent drafting for machine-generated work and is not a representation that copyright subsists. Taiga records the human contributions to each delivery in the audit trail, keeps that record for seven years and produces it on request.

8.2 The Platform is Taiga's

Taiga retains the Platform, its source, architecture, models, prompts, agents, evaluation harnesses, tooling, templates, scaffolding, reusable modules, processes and documentation. Taiga grants the Customer a perpetual, irrevocable, royalty-free, sublicensable licence to use, modify and exploit any Taiga background material to the extent embedded in Delivered Software. Taiga warrants that every employee, contractor and advisor who contributes has assigned present and future rights to Taiga in writing, with moral rights waived to the extent tekijänoikeuslaki 404/1961 permits.

8.3 Trade secrets, residuals and open source

Delivered Software, its specifications and its architecture are the Customer's trade secrets under liikesalaisuuslaki 595/2018 for as long as they remain secret, and Taiga does not disclose, reuse, publish or reference them without written consent. Taiga may use the general know-how its people retain in unaided memory and may improve its own templates and modules, provided nothing embodies the Customer's confidential information. The open-source components in a delivery are those declared in its dependency manifests; Taiga warrants that no GPL, AGPL, statically linked LGPL or SSPL component is incorporated so as to require disclosure of the Customer's source without prior written notice and acceptance, and scans and remediates the rest at its own cost on notice. The Platform does not generate a software bill of materials today; Taiga will deliver a machine-readable one from the date it publishes the capability and in any event with every delivery on or after 11 December 2027.

8.4 Feedback

Taiga may use feedback and bug reports for any purpose without obligation. This gives Taiga no right to Customer Content or Delivered Software.

9. IP INFRINGEMENT INDEMNITY

If your delivered software infringes someone else's rights in Europe, we defend you and fix it. It is capped, and it does not cover what you told us to build or what you changed.

Taiga defends the Customer against third-party claims that Delivered Software infringes an intellectual property right in the EU, the EEA, Switzerland or the United Kingdom, and pays amounts finally awarded or agreed in settlement. Taiga may procure the right, replace or modify the software so the infringement ceases, or failing that terminate the affected Service and refund fees for the affected period less actual use; that is the Customer's sole remedy. Liability under this clause is limited to the super-cap in clause 14.2 and to EUR 1,000,000, unless Special Terms state a higher ceiling. Conditions: prompt written notice, Taiga's control of the defence and settlement (the Customer may reasonably reject a settlement admitting its wrongdoing or imposing an ongoing obligation), reasonable co-operation, a Governed Run, no unapproved modification or combination, compliance with disclosed open-source obligations, and cessation of use on notice. Excluded: claims arising from the Customer's inputs, specifications or instructions, knowing infringement, the practice of a patented invention in an output, and use of an output as a trademark. Output may not be unique; the same or similar output may be produced for other customers.

10. CONFIDENTIALITY

Each Party keeps the other's confidential information confidential, uses it only for the Agreement, and discloses it only to people who need it and are bound to confidentiality. This does not cover information that is public without breach, already known, independently developed or lawfully received from a third party, or that must be disclosed by law, with notice where permitted. The obligation lasts five years after the Agreement ends, and for trade secrets for as long as they remain secret.

What we learn about each other stays between us, and trade secrets stay secret for as long as they are secret.

11. DATA PROTECTION

Schedule D is the data processing agreement under Article 28 of Regulation (EU) 2016/679: the Customer is controller, Taiga is processor. Customer Content is not used to train, fine-tune or benchmark any model, Taiga's or a third party's; model inference runs through Amazon Bedrock, and Taiga passes through the commitment it receives that inputs and outputs are not stored, shared with the model provider or used to train a base model. For personal data in software delivered into the Customer's own environment, Taiga is neither controller nor processor.

We process on your instructions, never train on your content, and are neither controller nor processor for personal data inside software running in your own environment.

12. SECURITY, INCIDENTS AND AUDIT

Taiga maintains the controls in Schedule B. Taiga notifies the Customer of a security incident or personal data breach affecting it without undue delay and in any event within twenty-four (24) hours of becoming aware, keeps the Customer informed until it is resolved and delivers a written root-cause report within thirty (30) days. The Customer may audit Taiga's compliance once per calendar year, and after an incident, on twenty business days' notice, during business hours, through itself or an auditor that is not a Taiga competitor; the Customer bears the cost unless the audit finds a material defect, in which case Taiga does. Any authority with supervisory powers over either Party has access as the law requires.

Schedule B says what we run and, just as plainly, what we do not yet have. We tell you about incidents within 24 hours and you can audit us once a year.

13. REGULATORY ROLES

Who is the AI Act provider, who is the CRA manufacturer, and what the new product liability rules mean. Short, because roles are fixed by law and this only allocates the work.

Taiga is the provider of the Platform as an AI system under Regulation (EU) 2024/1689 and the Customer is its deployer; the Customer becomes a provider only of an AI system it builds and places on the market itself. The Platform discloses that users interact with an AI system and that artefacts are AI-generated. Where the Customer becomes the provider of a high-risk AI system built on the Platform, Taiga supplies the information and technical access Article 25(4) requires, by written agreement and at the rates in the Rate Card. Each Party supports the development of AI literacy among its own staff. For Delivered Software the Customer places on the market, the Customer is the manufacturer under Regulation (EU) 2024/2847 and Taiga does not supply it under its own name; Taiga notifies the Customer of actively exploited vulnerabilities it detects within twenty-four (24) hours and supplies security updates for Delivered Software free of charge for the term of the Agreement, or a longer support period stated in Special Terms. Liability under the law implementing Directive (EU) 2024/2853 toward an injured person cannot be limited; between the Parties, Taiga is producer of the Platform and the Customer of the Delivered Software it places on the market or puts into service, and each gives the other prompt notice, evidence and cooperation on any claim.

14. LIABILITY

Twelve months of what you paid, capped in euros on your Order Form. Twice that for data protection, confidentiality and IP. Neither side pays the other's lost profits.

14.1 Cap

Each Party’s aggregate liability under or in connection with the Agreement is limited to the fees the Customer paid under the Order Form in the twelve (12) months before the event, and in no event exceeds EUR 1,000,000, unless Special Terms state a higher ceiling. Service credits under Schedule A are the sole financial remedy for availability shortfalls and count toward this cap.

14.2 Super-cap

Liability for breach of Schedule D or of data-protection obligations, for breach of confidentiality, and under clause 9 is limited to twice the amount in clause 14.1. One event never draws on more than one cap.

14.3 Indirect loss

Neither Party is liable for loss of production, turnover or profit, loss from inability to use, loss or corruption of data, damage to other property, or sums paid to third parties including contractual penalties, however arising.

14.4 Not limited

Nothing limits liability for wilful misconduct, gross negligence, death or personal injury, the Customer's obligation to pay fees, or anything mandatory law does not allow to be limited, including liability under the law implementing Directive (EU) 2024/2853.

14.5 Claims

A claim is notified in writing, stating its basis and, so far as ascertainable, its amount, within twelve (12) months of when the claiming Party found or should have found the circumstance, and proceedings begin within a further twelve (12) months. Claims for unpaid fees and trade-secret claims are outside this clause.

15. INSURANCE

One million euros on each of three policies, or more if your Order Form says so, running on for two years after the contract for work done during it.

Taiga maintains professional indemnity, cyber and product liability insurance, each with a limit of not less than EUR 1,000,000 per claim and in aggregate per insurance year or a higher minimum stated in Special Terms, for the term and — in respect of acts and events during the term — for two years after it. Taiga produces evidence of cover on request, once a year, and notifies the Customer if cover lapses or is materially reduced.

16. TERM AND TERMINATION

Rolling monthly both ways, or a 12-month term at 10% off that binds both of us. Non-payment costs you Deliver first, then Operate, and never your ability to get your data and code out.

16.1 Rolling monthly

The Agreement runs from the effective date on the Order Form on a rolling monthly basis. Either Party may terminate it, or either rail, with effect from the end of the calendar month following the month in which notice is given.

16.2 Committed term

Where the Order Form records a twelve-month committed term: the Learn fee and the base Deliver + Operate fee are ten per cent (10%) lower for every month and the Order Form states them net; fees, steps and the Rate Card version are frozen, though Aurora continues to track actual consumption as clause 4.6 provides; the recorded steps are the floor, so the Customer may step up (at list fees) but not down; Taiga may not terminate for convenience before the term ends; if the Customer terminates for convenience early, the discounted fees for the remaining months fall due — never where it terminates under clause 16.5, clause 17, Schedule B, for Taiga's material breach or under any other right the Agreement gives it; and at the end of the term the Agreement continues monthly at the fees then in force, without automatic renewal, with any renewal increase capped at the greater of five per cent and the change in the Finnish consumer price index and notified with reasons ninety (90) days ahead. An early-termination charge is not a switching charge.

16.3 Non-payment

Where an undisputed invoice is unpaid, Taiga reminds the Billing Administrator in writing and, not less than thirty (30) days later, may suspend Deliver, then Operate, and — only in Taiga-hosted mode and after a further thirty-day read-only period — the runtime, or terminate. Suspension of Deliver never suspends a paid Learn rail. Data export, code mirroring and switching assistance survive every step and are never conditioned on payment. Taiga never suspends or disables Delivered Software running in the Customer's own cloud account.

16.4 Immediate suspension and breach

Taiga may suspend access without prior notice, no more than the situation requires and with notice as soon as lawful, for a genuine security threat, unlawful use, legal compulsion or an Acceptable Use Policy breach that endangers other tenants. Either Party may terminate for a material breach not remedied within thirty (30) days of written notice.

16.5 Chronic availability failure

Where the availability target is missed in three consecutive months or four months in any twelve, the Customer may terminate the affected Service on thirty (30) days' notice, without charge, within sixty (60) days of the last month counting.

16.6 On termination

Access ends; fees accrued remain payable; Schedule C governs export, switching and erasure; and clauses 5.1 (for output already in production), 8, 9, 10, 11, 13 (for the support period), 14, 15 (for its period), 16.2 (for a charge fallen due), 16.3 (last two sentences), 18 and 19 survive.

17. CHANGES

We change the platform constantly. A change that hurts you gets 30 days' notice and a free exit; a security fix or a legal requirement does not wait.

Taiga may change the Services and these terms on thirty (30) days' written notice. Where a change is materially adverse to the Customer, the Customer may terminate the affected Service without charge from the date the change takes effect. Changes required by mandatory law, security fixes and changes that do not materially reduce functionality or the Customer's rights take effect on notice.

18. GENERAL

The housekeeping: who can take over the contract, what happens if we are acquired, and where notices go.

Assignment. Neither Party assigns the Agreement without the other's written consent, not unreasonably withheld for an intra-group transfer or a transfer with the business. Taiga may assign or pledge its receivables to a bank or financial institution for financing on written notice; payment to Taiga discharges the Customer until it receives that notice, set-off and defences are preserved, and the assignee is bound by clause 10.

Change of control. Each Party notifies the other of a change of control. The Customer may terminate on thirty (30) days' notice, within sixty (60) days of notice, where a direct competitor of the Customer — an undertaking supplying, in competition with the Customer, the principal products or services the Customer supplied at the date of the Order Form — acquires control of Taiga. An intra-group reorganisation or a financing round that does not change control is not a change of control.

Subcontracting. Either Party may use subcontractors and remains liable for them; subprocessors of personal data are governed by Schedule D.

Notices and invoicing details. Notices go in writing to hello@tai.ga for Taiga and to the email address of the Customer's administrator recorded in the Platform for the Customer; email is received on the next business day absent a bounce; termination, suspension and claim notices also go by registered post to the registered address. The Customer's invoicing address and e-invoicing details are maintained by its administrator in the Platform.

Force majeure. Neither Party is liable for failure caused by an event beyond its reasonable control; either may terminate if it lasts more than sixty (60) days.

Publicity. Taiga may name the Customer and use its logo as a reference only with the Customer's written permission.

Other. Invalid provisions are severed; no waiver is implied from forbearance; no third party has rights; the Agreement is the entire agreement and is executed by eIDAS-compliant electronic signature (Regulation (EU) 910/2014) in counterparts; each signatory warrants authority; English governs.

19. LAW AND DISPUTES

Finnish law. Unpaid invoices go to the Helsinki court, small metering disputes to an expert, everything else to arbitration in Helsinki.

The Agreement is governed by Finnish law, excluding its conflict-of-laws rules and the CISG. A claim for an undisputed debt may be brought in the District Court of Helsinki or by summary proceedings. A metering or invoicing dispute below EUR 50,000 goes to binding determination by an independent expert the Parties agree on, each bearing its own costs and half the expert's fee, or failing agreement within fifteen business days, to arbitration. All other disputes are finally settled by arbitration under the Arbitration Rules of the Finland Chamber of Commerce, seat Helsinki, language English; the Expedited Rules apply where the amount in dispute is at or below EUR 100,000, and either Party may ask the Institute to apply the full Rules having regard to the amount, complexity and other relevant circumstances.

SCHEDULE A. SERVICE LEVELS AND SUPPORT

One region, several availability zones, an honest number per step, and money off the invoice when we miss it. Response times, never resolution times.

Scope. The availability commitment covers the Taiga control plane. It does not cover the Customer's GitHub or cloud account, Delivered Software running in the Customer's environment, model inference and Amazon Bedrock availability, the quality of agent output, preview features or time in Action Required. Failure of the infrastructure Taiga runs on is not excluded; force majeure is.

Target. Taiga commits to the monthly availability target the Service Description states for the Customer's step; the target follows the step. Availability is measured per calendar month as the Service Description states. Planned maintenance announced in advance within the limits the Service Description states is excluded, as is emergency security maintenance notified as soon as practicable. Taiga provides the monthly figure on request. The target is a commitment, not a claim about past performance; Taiga runs in one EU region across several availability zones and a region-wide failure can exceed any target.

Credits. A shortfall earns a service credit against that month's fee for the affected rail, at the rate the Service Description states for the size of the shortfall. Credits are claimed in writing within thirty (30) days of the month or of receiving the figure, are applied to the next invoice or paid where none follows, never exceed the month's fee for the rail, are not Aurora, and are the sole financial remedy for availability shortfalls. Repeated failure gives the exit in clause 16.5.

Support. Support is included on every step. Hours, priority levels and response targets are those the Service Description states. Targets are response targets, never resolution targets. Assistance beyond support is agreed in writing before the work.

SCHEDULE B. SECURITY AND ASSURANCE STATUS

What we run, and what we do not yet have, in the same words as tai.ga/en/trust. If a certificate is not held, this says so.

Where the Platform runs. AWS eu-central-1 (Frankfurt), with the application and database tiers across more than one availability zone and backups in a separate isolated account under its own key. Model inference runs through Amazon Bedrock in EU regions; Bedrock may serve a request from another EU region for capacity, persisting nothing, and the TLS certificate in front of the service is managed in a US region, which is certificate metadata and never Customer Content. Non-EU regions are denied by organisation-wide policy at the infrastructure boundary.

Controls. Taiga maintains the technical and organisational measures described at tai.ga/en/trust as at the date of the Order Form, and at all times at least: tenant isolation enforced at the data layer; encryption in transit and at rest, with customer-managed keys for uploaded content; operator access only through single sign-on with multi-factor authentication and no standing database access; agents on a private network under least privilege, reaching the Customer's repositories only through the App the Customer installs and within execution limits; security scanning of every change and continuously in operation; and infrastructure managed as peer-reviewed code. Vulnerabilities in the Platform are remediated within the targets the Service Description states.

Retention. Account and project data for the life of the Agreement; database point-in-time backups 30 days; superseded uploaded document versions 30 days; control-plane audit logs seven years in an isolated immutable archive; operational logs 365 days. Backup and recovery of the Customer's own repository and cloud account are the Customer's in Customer-hosted mode; Taiga tests restoration of Platform data and records the result.

Subprocessors for the Platform. Amazon Web Services EMEA SARL (infrastructure, database, storage, identity, model inference, email; EU, eu-central-1); Anthropic, reached only through Amazon Bedrock as model supplier, receiving no prompts, responses or service logs; GitHub (repository access through the Customer-installed App); Google (optional single sign-on, and developer-documentation lookups by agents that carry the question, not the Customer’s code and no personal data); Microsoft (optional Entra ID single sign-on, claims in transit only). Changes are notified under Schedule D.

Assurance status. The information security management system is established and operating, aligned to ISO/IEC 27001:2022; ISO/IEC 27001 certification is in progress and not held; SOC 2 Type II is planned and not held; no third-party penetration test has been carried out; two Amazon Bedrock Guardrails profiles are built and versioned but switched off in every environment, including production, while support cases with AWS remain open — the controls above carry the surface. Where Taiga has committed in writing to a target date for a milestone and it is missed, Taiga notifies the Customer, agrees a revised date, commissions an independent assessment at its own cost if the revised date is missed, and the Customer may terminate the affected Service without charge if the milestone is more than 180 days late. Nothing in the Agreement states or implies a certification, a completed test or an enforcing control that this Schedule records as not held.

SCHEDULE C. EXIT AND SWITCHING

Your code is already in your own repository, switching is free, and the timetable is the one the EU Data Act requires.

Right to switch. The Customer may at any time, by written notice, switch to another provider, to its own premises or to running both in parallel. The notice period to initiate switching never exceeds two months; a transitional period of at most thirty (30) calendar days follows, during which Taiga maintains continuity and security and discloses known risks, and which the Customer may extend once; where thirty days is technically unfeasible Taiga says so within fourteen working days with reasons and an alternative period of at most seven months; a data-retrieval period of at least thirty (30) calendar days follows the transitional period; then erasure. These provisions implement Chapter VI of Regulation (EU) 2023/2854.

No switching charges. Taiga makes no switching, egress or migration charge, from the effective date of these terms and as Article 29 of that Regulation requires from 12 January 2027. Ordinary monthly fees continue through the notice and transitional periods, and an early-termination charge under clause 16.2 is not a switching charge. Taiga is not liable for loss arising from the switching or deletion process itself, and the Customer indemnifies Taiga against claims by its own affiliates and users arising from an instruction it gives.

What is exportable. In Taiga-hosted mode: repositories and source, infrastructure definitions, CI/CD definitions, the Discovery documents, TaigaSense findings, delivery metrics, deployment history, the tenant audit trail, uploaded document versions and a tenant database export. In Customer-hosted mode the Customer already holds its code and infrastructure; Taiga exports the control-plane data it holds — Discovery documents, findings, metrics, deployment history, audit trail, uploaded documents. Everything not listed is exportable by default; withheld on trade-secret grounds, with written justification, are only model prompts, agent definitions, model routing, evaluation harnesses and cross-tenant operational telemetry, and withholding them never impedes switching. Export is self-service in the Platform, in structured, commonly used, machine-readable formats, and remains available for thirty (30) days after termination.

Erasure and continuity. A tenant owner instructs erasure in the product; a thirty-day cancellable grace period follows during which the tenant stays usable; erasure completes within thirty-five (35) days with a signed deletion certificate, subject to the retention in Schedule B and any legal hold. In Customer-hosted mode there is nothing to escrow: the Customer loses the Platform, not the product. In Taiga-hosted mode, source and deployment configuration are mirrored to the Customer continuously through the term, and Taiga hands over the runtime environment on switching.

SCHEDULE D. DATA PROCESSING

The GDPR Article 28 terms: your instructions, our subprocessors, 24-hour breach notice, EU processing, and what we keep after erasure and why.

Roles and scope. The Customer is controller and Taiga processor of the personal data in Customer Content. Taiga processes only on the Customer's documented instructions — this Agreement, the Order Form, the configuration the Customer sets and instructions its authorised personnel give — and informs the Customer if an instruction infringes data-protection law. Taiga is neither controller nor processor for personal data in software delivered into the Customer's environment. This Schedule prevails over the rest of these terms on personal data but does not enlarge liability beyond clause 14.

Taiga's obligations. Persons authorised to process are bound to confidentiality; the technical and organisational measures are those in Schedule B; Taiga assists the Customer, taking account of the nature of processing, with data-subject requests and with Articles 32 to 36 of Regulation (EU) 2016/679; at the end of the Services Taiga deletes or returns personal data at the Customer's choice, subject to the retention below; Taiga makes available the information necessary to demonstrate compliance and contributes to audits under clause 12.

Subprocessors. The Customer authorises the subprocessors listed in Schedule B and gives general written authorisation for others. Taiga notifies an intended addition or replacement before it takes effect; the Customer may object on reasonable grounds within thirty (30) days; the Parties then seek a solution in good faith and, failing one, the Customer may terminate the affected Service without charge. Taiga imposes equivalent data-protection obligations on each subprocessor and remains fully liable for them. Where the DORA Add-on applies, its subcontracting consent rights override this paragraph.

Breach notification. Taiga notifies the Customer without undue delay and in any event within twenty-four (24) hours of becoming aware of a personal data breach, with the nature of the breach, the categories and approximate numbers of data subjects and records, the likely consequences and the measures taken, updates daily until resolved and reports on root cause within thirty (30) days. The Customer decides on notification to the supervisory authority and to data subjects.

Location and transfers. Personal data is processed in the EU or EEA; Bedrock may process a request in another EU region without persisting it. Taiga does not transfer personal data outside the EU or EEA without the Customer's prior written consent and safeguards under Chapter V. For any residual transfer — optional Google or Microsoft single sign-on, agent documentation lookups, support — the Standard Contractual Clauses in Commission Decision (EU) 2021/914 are incorporated as the fallback mechanism, with a transfer impact assessment and pseudonymisation as a supplementary measure, and engage automatically if an adequacy decision is annulled, suspended, adversely amended or put under review.

No training. The Customer instructs, and Taiga confirms, that Customer Content and personal data are not used to train, fine-tune, adapt or benchmark any model, Taiga's or a third party's. Metering, error and performance telemetry containing no Customer Content and no personal data is used to operate, secure and improve the Services, and nothing else derived from the Customer's use is.

Retention after erasure. Erasure follows Schedule C. Control-plane audit logs (user identifier, action, timestamp) are retained for seven years in an isolated immutable archive on the bases of legal retention where a law applies, the establishment and defence of legal claims, and the integrity of the audit trail, with Taiga as controller of that record; residual encrypted backups age out within thirty-five days; a legal hold suspends erasure.

Description of processing. Data subjects: the Customer's personnel and contractors who use the Platform, and persons whose data appears in Customer Content. Categories: identifiers, contact details, professional data, account and usage data, and any personal data the Customer includes in repositories, specifications or documents. Purpose: providing the Services. Duration: the term of the Agreement and the retention above. Location: EU, eu-central-1. The Customer does not introduce special-category data or sector-secrecy data without a written addendum.