firmfact

Terms and Conditions

Firmfact Customer Legal Package

DOCUMENT CONTROL

VERSION
v2026-Q3

BUILD
2026-Q3.e0e12a6

PUBLISHED
10 August 2026

CLASSIFICATION
Customer-Facing

DISTRIBUTION
Enterprise customers, prospects, auditors

© 2026 Dutchcode B.V.
Governed by Dutch law

Last updated: 10 August 2026

Purpose Of These Terms

These Terms and Conditions form the core master agreement for the use of firmfact. They apply to the B2B SaaS services provided by Dutchcode B.V. trading as Firmfact to business customers using the platform for spend management, contract management, document processing, and related workflows.

We do not use your Account Data to train, fine-tune, or improve any machine-learning or AI model. AI-assisted features process your content only to provide, secure, support, and troubleshoot the requested functionality in accordance with the Agreement and DPA, as described in the AI Features And Processing Boundaries section below.

These Terms And The Rest Of The Agreement

Capitalised terms have the meaning given where they are defined in bold in the text or in Defined Terms at the end.

What forms the Agreement. The Agreement is these Terms together with, where each applies: the DPA, including its appendices and any incorporated transfer annexes; the SLA; the Commercial Terms recorded for a Subscription; and any negotiated addendum expressly incorporated into the parties' contract.

If Customer uses the Service to process personal data for which Dutchcode B.V. acts as processor, the DPA applies automatically and forms part of the Agreement regardless of plan tier.

The SLA applies only to a paid Subscription expressly designated as SLA-eligible in the Commercial Terms. **Free Tier** (the default no-fee plan), **Trial** (a temporary evaluation period for a paid feature or plan), **Demo Account** (a non-production Account for evaluation, configuration, testing, training, or demonstration), and **Beta Features** (beta, preview, pilot, or early-access features) are excluded unless expressly stated otherwise. Where the SLA applies, service credits are Customer's sole and exclusive monetary remedy for failure to meet the uptime commitment. The SLA is not published as a general website download for anonymous visitors: where it applies, it is made available through the documented acceptance workflow and, after onboarding, through Customer's account Trust Centre.

The **Privacy Notice** published for firmfact is notice of controller-side processing. It is acknowledged as part of the legal package but does not by itself create independent contractual remedies unless a specific provision is expressly incorporated into the Agreement.

How the Agreement is formed. The Agreement may be formed through one or more documented acceptance events. Free Tier users accept the legal package through clickwrap at signup or first Account creation, covering these Terms and, where applicable, the DPA. For Paid Plans, including **Professional Plan** and **Enterprise Plan**, the DPA and, where applicable, the SLA form part of the Agreement when accepted through any documented acceptance event. A negotiated or regulatory overlay applies only where an executed Order Form or addendum expressly says so.

The applicable legal package may be recorded through clickwrap, account creation, an in-product subscription agreement workflow, upgrade flow, feature enablement, Order Form, or another documented legal event. The recorded acceptance event may include the accepted document set, package hash, commercial selections, signatory details, timestamp, tenant and user identifiers, and assent text shown in the workflow. Generated PDFs and rendered snapshots are evidence artifacts of that documented legal event and do not by themselves constitute separate signature workflows.

Where a Paid Plan is accepted through an in-product **Subscription Agreement** workflow, the acceptance record also captures the selected plan, billing cadence, first invoice date, payment term, and the technical details of the acceptance event, including the originating IP address. These records exist so both parties can later prove what was agreed and when.

Customer purchase orders, procurement portal terms, onboarding terms, click-throughs, supplier-registration forms, and similar customer-provided paper are administrative only and do not amend or supplement the Agreement unless expressly accepted in writing by an authorised signatory of Dutchcode B.V. trading as Firmfact.

Only the Agreement and executed addenda create binding contractual commitments. Security questionnaires, policy suites, architecture diagrams, business continuity summaries, accessibility statements, automated scan outputs, and similar diligence materials are informational only unless an Order Form or addendum expressly incorporates them.

Order of precedence. If there is any conflict among the documents forming the Agreement, the following order of precedence applies, highest first:

- any negotiated addendum expressly incorporated into the parties' contract, but only for the matters it expressly addresses;
- the applicable Order Form or Subscription Agreement, but only for commercial terms, plan-specific terms, and other matters it expressly addresses;
- the DPA, but only for data protection, privacy, data transfer, and processor obligations;
- the SLA, but only for service levels, support commitments, and service credits;
- these Terms;
- the Privacy Notice as notice and other referenced policies or diligence materials, unless expressly elevated in an Order Form or addendum.

Commercial Terms rank with the Order Form and the Subscription Agreement in that order of precedence, and therefore prevail over the default positions in these Terms for the matters they expressly record. These Terms do not repeat that point clause by clause.

Your Data

Customer Organisation owns it. Customer Organisation retains all right, title, and interest in and to Account Data.

We do not sell it. We do not sell Account Data, and we do not share Account Data for advertising or marketing purposes.

Our licence is limited to running the Service. Customer Organisation grants us a non-exclusive, worldwide, limited-term right to use Account Data only as necessary to provide, secure, support, maintain, and operate the Service and to perform our obligations under the Agreement. Within that limit, the right covers hosting, storing, copying, backing up, transmitting, processing, indexing, securing, supporting, maintaining, troubleshooting, and otherwise using Account Data. Access to Account Data by our personnel is limited to individuals who need it for those purposes and is subject to the confidentiality obligations set out under Confidentiality; Account Data is Confidential Information of Customer Organisation.

It stays in the EU. Account Data is hosted in EU data centres. We will not move hosting of Account Data outside the EU / EEA without prior notice to Customer, and any such change is subject to the material-change provisions of these Terms and to the DPA. This commitment applies to all Account

Data, whether or not it constitutes personal data; where the data is personal data, the DPA's international-transfer provisions also apply.

Accounts are kept separate. We maintain access controls and Account-scoping measures designed to keep each Account's Account Data separate from every other Account's, so that Account Data is not made available to another customer through the Service. Those measures are described in the technical and organisational measures in the DPA.

Legal demands. If we receive a legal demand for Account Data, we will disclose only what is legally required and, wherever the law permits, give Customer prompt notice so it can seek confidential treatment or a protective order. The full commitment is under Confidentiality, because Account Data is Confidential Information.

Aggregate usage statistics. We may use de-identified and aggregated data derived from Customer Organisation's use of the Service only for non-AI internal service improvement, reliability, capacity planning, security, and operational analytics, provided that such data does not identify Customer Organisation or any individual and cannot reasonably be re-identified. Such data is not used to train, fine-tune, or improve any machine-learning or AI model. We will not publicly identify Customer Organisation, or use such data for public comparative benchmarking against Customer Organisation, without its express written consent.

Export. Customer Organisation may export Account Data using the available export tools or other agreed export mechanisms during the subscription term and any offboarding period. The standard in-product export package is a machine-readable current-state snapshot of Account Data, the **Account Audit Trail** (the customer-accessible history of actions and access activity for an Account) for the selected export scope, referenced files, and manifest/checksum metadata, delivered through authenticated download flows in the standard formats the Service provides, including CSV and JSON where supported. An export covers Account Data and its audit trail rather than a copy of our own operating records, so unless expressly stated otherwise it does not include **Internal Security Logs** (our provider-side operating, security, and diagnostic records) or every other provider-side record maintained by firmfact.

Unless an Order Form states otherwise, Customer will have up to 180 days after termination or expiration to complete exports before ordinary deletion workflows are carried out.

Deletion. Deleting, disabling, or removing a User does not by itself cancel a Paid Plan, terminate the Agreement, delete an Account, or delete records retained under the paragraph below.

When the Agreement ends, Account Data is deleted through our ordinary deletion workflows after the export period described above. Where Account Data contains personal data, the DPA's deletion timetable applies. A few categories outlive that, and only where legally, operationally, or contractually required:

- financial, billing, and tax records, for the applicable Dutch statutory retention period;
- Account Audit Trail records, where legally or contractually required;
- Internal Security Logs, where legally, operationally, or contractually required;
- backup data, until it ages out of the ordinary backup retention cycle.

Indicative retention periods are set out in the Retention, Export, And Deletion section of the Privacy Notice, and retention and deletion of personal data are governed by the DPA.

AI Features And Processing Boundaries

AI-assisted processing is part of how the Service works rather than a feature Customer switches on. Automated extraction turns an uploaded contract or invoice into structured data, so it runs whenever a document is uploaded; other AI-assisted features process Account Data when Customer uses them. In each case Account Data is processed for that purpose by our AI subprocessor, which is identified, together with its location and the retention limits that apply to it, in the Privacy Notice and in the processor-side subprocessor register. Where Account Data is processed by AI-assisted features:

- we will **not** use Account Data, including de-identified or aggregated derivatives, to train, fine-tune, or improve any machine-learning or AI model, and we will not instruct or authorise any subprocessor or third party to do so. This applies for as long as we hold any Account Data, including after termination and while Account Data remains in backups;
- Customer Organisation retains ownership of Account Data submitted as prompts, documents, or other AI inputs;
- Customer owns Customer-specific outputs generated for Customer through the Service to the extent permitted by applicable law and the rights of relevant third-party model providers, subject to our ownership of the Service itself;

- we process Account Data through AI-related subprocessors strictly to provide, secure, support, and troubleshoot the requested functionality in accordance with the Agreement and DPA;
- Customer remains responsible for reviewing outputs before relying on them for business, legal, operational, or compliance decisions. AI-generated outputs assist workflows and may contain errors, omissions, or incomplete inferences.

EU AI Act posture. For the AI-assisted features made available through the Service, Dutchcode B.V. acts as a **deployer** of AI systems under Regulation (EU) 2024/1689 (the "EU AI Act") and not as a provider of general-purpose AI models. Foundation-model provider obligations, including the transparency and systemic-risk obligations applicable to general-purpose AI model providers, rest with the relevant upstream subprocessor. The Service is not designed for, and Customer shall not use the Service for, any practice prohibited under Article 5 of the EU AI Act. Where Customer's own use of the Service for a specific workflow would qualify as a high-risk AI system under Annex III of the EU AI Act, Customer remains responsible for the corresponding deployer obligations that attach to that use.

Security, Operational Resilience, And DORA

We maintain security and operational resilience measures appropriate to the nature of the Service. Data residency and Account separation are addressed under Your Data.

We may carry out planned and emergency maintenance and make reasonable changes to the Service's infrastructure, hosting architecture, APIs, and technical and security configuration where necessary to maintain security, legal compliance, performance, resilience, or operability. Changes to hosting architecture remain subject to the data-residency commitment given under Your Data. Where commercially reasonable, we will give prior notice of planned maintenance or material changes, and the material-adverse-change provisions of these Terms and any applicable SLA or Order Form continue to govern where a change materially reduces contracted functionality.

We may satisfy ordinary security assurance requests through our then-current evidence package, questionnaires, and reasonable remote review discussions in the first instance. We do not make commitments in these Terms regarding certifications, formal attestations, manual penetration testing, or audit rights beyond what is expressly stated in the Agreement or supported by our current evidence package. Where Customer requires a specific certification, attestation, or testing programme, the parties may agree it in an Order Form. Any audit, information, or assistance rights

that apply under the DPA remain governed by the DPA and are not reduced by plan tier.

Enterprise assurance and regulated outsourcing. For **Enterprise Plan** customers, and for other customers only to the extent expressly stated in an Order Form, we will provide the cooperation described in the rest of this section. These are **Enterprise Services** and do not apply to other plans by implication.

Enterprise Plan customers may request one scoped audit or control review in any 12-month period where legally required, reasonably necessary for Customer's regulated outsourcing compliance, or where the evidence package is materially insufficient for the requested review. Any such audit must be conducted by an independent, confidentiality-bound, non-competitor auditor on reasonable prior notice, during normal business operations, and in a manner that minimises disruption and protects the security of the Service and other customers. Customer bears audit costs unless the audit identifies a material non-compliance with an express contractual commitment. Nothing in this section prevents a broader review by a regulator or competent authority where applicable law requires it, subject to reasonable confidentiality, security, privilege, and operational protections.

We will also provide the baseline operational-resilience and regulated-outsourcing cooperation reasonably necessary for Customer's compliance as it relates to the Service:

- notice without undue delay after confirmation of a material operational or security incident materially affecting the Service, with reasonable follow-up updates during active mitigation;
- reasonable advance notice of material subcontracting changes and material hosting or delivery-structure changes relevant to Customer's regulated-outsourcing obligations, except where a shorter timeline is required for urgent security, legal, or operational reasons;
- reasonable cooperation with Customer's outsourcing register, concentration-risk review, business continuity review, and exit planning requirements as they relate to the Service.

Personal data breach notifications remain governed by the DPA, which applies regardless of plan tier. Providing this baseline is not by itself a change order; customer-specific templates, bespoke questionnaires, regulator-directed projects, and work beyond it remain subject to an Order Form, addendum, or change order.

If the parties execute a negotiated or regulatory addendum, that addendum governs the matters it expressly addresses and prevails over this section to the extent of any inconsistency.

Plans, Accounts, And Non-Production Use

The Service is offered as Free Tier, Professional Plan, Enterprise Plan, Trial, and Demo Account. In the product and on the pricing page these appear under marketed names: **Starter** is the Free Tier, **Professional** is the Professional Plan, and **Enterprise** and **Enterprise Plus** are both Enterprise Plans, Enterprise Plus being a distinct marketed tier with its own capacity ladder. "Unlimited" (or equivalent) is a capacity step within that ladder, not a synonym for Enterprise Plus.

Unless an Order Form states otherwise, new signups may receive a **Production Account** (the Account designated for ordinary operational use) and a Demo Account where that onboarding path is available, and all Accounts start on the Free Tier. A Customer Organisation may maintain multiple Accounts, and unless expressly stated otherwise in writing each Subscription applies only to the Account for which it was purchased or activated.

Plan-specific entitlements. Numerical usage limits, included features, support tier, support coverage window, initial response targets, SLA eligibility, SSO / OIDC availability, API and **MCP** (machine-readable agent interface) access, enterprise assurance rights, regulated-outsourcing support, and premium support or resilience commitments are determined by the selected plan as recorded in the Commercial Terms, and are subject to the scope, rate limits, authentication requirements, and acceptable-use restrictions applicable to that access. No feature, support level, assurance right, or regulatory cooperation obligation applies across plans by implication. In particular, unless expressly included in an Order Form, the Professional Plan does not include Enterprise Services, regulated-outsourcing support, scoped audit or control-review access, or premium incident-response handling beyond the standard paid-plan SLA and support commitments.

Purchased limits are enforced, not billed. The usage limits recorded in the Commercial Terms are enforced as Customer works: when a limit is reached, the Service declines the further action rather than quietly allowing it and charging for it afterwards. Exceeding a purchased limit does not generate additional charges. If an Order Form expressly defines an overage rate or other overage mechanism for a limit, that Order Form governs excess usage for that limit instead.

Reaching a limit does not switch the Service off. The Account stays available and Customer keeps working with the data already in it, including viewing, editing, reporting, and export. Only the metered activity itself pauses: document processing and AI-assisted features, until the next billing period or an upgrade; and adding users or tracked entities beyond the purchased licence count, until additional capacity is purchased or an upgraded plan is selected. The Service shows usage against

each limit in the Account and flags a limit as it is approached, so a limit should not arrive unannounced. Where sustained overuse creates a genuine service or security risk, the suspension rights under Suspension And Termination still apply.

Non-production and pre-release use. Trials, Demo Accounts, and Beta Features are provided on an AS-IS basis. Free Tier, Trials, Demo Accounts, and Beta Features are excluded from uptime commitments, service credits, recovery objectives, and support response or resolution commitments, unless expressly stated otherwise in an Order Form. Beta Features may also be changed or withdrawn at any time.

Free Tier hibernation. If a Free Tier Account has no team activity for **90 consecutive calendar days**, we may place it in read-only hibernation. We email account administrators **7 calendar days before** hibernation begins (when inactivity reaches 83 days). In hibernation, Customer may still sign in, view existing data, and export reports where the Service permits, but may not create or change records until a team member resumes activity or Customer upgrades to a Paid Plan. Any team member's sign-in or continued use restores full access immediately unless the Account is otherwise restricted for billing or security reasons.

Subscription Term, Renewal, And Changes To The Service

Free Tier access continues until terminated under these Terms or discontinued by Customer through the available cancellation workflow.

Paid Plans renew automatically for successive periods equal to the then-current Commitment Term unless Customer gives at least 30 days' prior notice of non-renewal through the designated in-product billing workflow or by written notice to legal@firmfact.com, unless an Order Form or Subscription Agreement states a different renewal term, notice deadline, or cancellation method. Customer may terminate a Subscription for convenience only effective at the end of the then-current Commitment Term, unless the Commercial Terms expressly provide an earlier termination right. Billing cadence does not shorten the Commitment Term, and merely stopping use of the Service does not itself stop billing. Where Customer holds more than one Subscription, terminating one does not by itself terminate the others; termination of the Agreement as a whole is dealt with under Suspension And Termination.

Reminder features, notice-tracking dashboards, renewal summaries, and similar workflow tools are administrative convenience features only. Customer remains responsible for monitoring its own notice deadlines, renewal decisions, cancellation actions, and other contractual milestones unless

the parties expressly agree otherwise in writing.

Changes to the Service. We may generally modify, replace, or deprecate Service features in the ordinary course of operating the Service. Where commercially reasonable, we will provide prior notice for changes that materially affect Customer's use of the Service. During a paid subscription term, however, we will not materially reduce core contracted functionality unless we provide substantially equivalent replacement functionality or Customer has the termination right described below.

If we make a material adverse change to the Service, pricing model, or usage metric that materially reduces Customer's contracted functionality or materially increases Customer's recurring charges, or if we materially reduce core contracted functionality during a paid subscription term without providing substantially equivalent replacement functionality, we will provide at least 30 days' prior notice. Customer may terminate the affected subscription by written notice given before the change takes effect. Unless Customer expressly agrees earlier or the change is required by law, the change will apply no earlier than the next renewal or billing period after the notice period has expired, and we will not charge the changed price for any period after a valid termination takes effect.

Fees, Invoicing, And Payment

Customer must provide accurate billing, tax, and contact details and keep them current. Unless the Commercial Terms state otherwise:

- usage is measured during the applicable billing month;
- invoices are issued according to the plan cadence recorded in the Commercial Terms;
- payment is due within 30 days of invoice date (Net 30);
- fees are non-refundable except where required by applicable law or expressly stated in an Order Form;
- fees are exclusive of VAT and other applicable taxes, which Customer must pay unless it provides a valid exemption or reverse-charge basis;
- we may change pricing or usage metrics on at least 30 days' prior notice for prospective billing periods, and any change applies only from the next renewal or billing period after the notice period expires.

Unless an Order Form states otherwise, any recurring subscription price increase for a standard plan will not exceed the lower of the then-current Consumer Price Index for all households as published by Statistics Netherlands (CBS) and 5% in any 12-month period.

Invoices may be issued through our invoicing and accounting providers, based on the applicable plan, measured usage, and any relevant Order Form. Customer must notify us of billing disputes in good faith within 60 days after invoice date. Customer may not withhold, set off, or suspend payment obligations except to the extent required by applicable law or expressly stated in an Order Form, and a good-faith dispute does not relieve Customer of the obligation to pay any undisputed amount when due.

Undisputed overdue amounts accrue statutory commercial interest under Dutch law (including the statutory commercial interest rate under Article 6:119a of the Dutch Civil Code, as applicable) from the due date until paid. Customer must also reimburse reasonable collection costs, including reasonable third-party recovery costs, incurred in collecting undisputed overdue amounts.

Non-payment of undisputed fees is handled as set out under Suspension And Termination.

Customer Responsibilities

Customer is responsible for:

- Users' compliance with the Agreement, and maintaining accurate account information;
- provisioning and deprovisioning Users, and assigning appropriate roles, permissions, and Account access scope for Customer Organisation's internal control environment;
- protecting credentials and access methods, maintaining password hygiene where password authentication is used, and configuring integrations, identity providers, MFA, SSO, and security settings correctly;
- providing timely, accurate, and complete information, materials, approvals, and decisions reasonably required for onboarding, support, integrations, security reviews, migration work, or other agreed services;
- designating personnel with appropriate authority and knowledge to make operational, technical, security, and commercial decisions on Customer's behalf;

- obtaining and maintaining cooperation, permissions, and access from Customer-managed third parties, systems, and providers where needed for the Service or any agreed project work; and
- validating that Customer's use of the Service is lawful and appropriate for its business.

Firmfact is not responsible for failures, delays, degraded performance, or access issues caused by Customer misconfiguration, Customer-managed identity providers, Customer-side role assignment or access-control choices, Customer-side integrations, unsupported third-party dependencies, misuse, abuse, or breaches of the acceptable use restrictions.

Firmfact is entitled to rely on authorised Account administrator instructions and Customer Organisation configuration choices, and Customer Organisation remains responsible for ensuring that assigned roles and access rights are appropriate for its own governance, segregation-of-duties, and regulated-environment requirements.

Where SSO / OIDC-based sign-in is included in the applicable plan or Order Form, Customer remains responsible for the availability, configuration, and security of its own identity provider. If the SLA applies, only firmfact-operated SSO / OIDC endpoints are covered to the extent expressly stated in the SLA.

If Customer delays or fails to provide required information, approvals, access, dependencies, or third-party cooperation, any resulting delay, degradation, or inability to perform is excused to the extent caused by that failure. Timelines may be extended, milestones may shift, and additional work caused by the delay or deficiency may be charged at the applicable contracted or then-current rates.

Acceptable Use

Customer and its Users must not:

- use the Service in violation of applicable law or regulation;
- upload or transmit unlawful, infringing, fraudulent, or malicious material;
- interfere with, disrupt, probe, or attempt to gain unauthorised access to the Service or related systems;
- reverse engineer, decompile, or attempt to derive source code except to the extent such restriction is prohibited by law;
- scrape, spider, mine, bulk extract, harvest, or index the Service, the Documentation, or other non-public materials made available by us, whether manually or by automated means, except through expressly authorised APIs or export tools;
- use the Service, the Documentation, or other non-public materials made available by us to create datasets, benchmarking corpora, or training material for machine-learning or AI models, to train or improve machine-learning or AI systems intended for external use, or to build or benchmark a competing service, except as expressly permitted by us in writing;
- publish Service performance, security, or benchmark testing results without our prior written consent, unless disclosure is required by applicable law or to a regulator, supervisory authority, external auditor, or professional adviser acting under confidentiality obligations;
- resell, sublicense, timeshare, or provide access to unauthorised third parties except as expressly permitted by the Agreement;
- use the Service in a manner that creates security risk, service abuse, or operational instability.

These restrictions do not reduce Customer Organisation's ownership rights in Account Data or Customer Organisation-specific outputs to the extent expressly granted elsewhere in the Agreement. Suspension or restriction of access for security, abuse, or legal-compliance reasons is dealt with under Suspension And Termination.

Support, Offboarding, And Extra Work

Except as expressly stated in the applicable SLA or Order Form, support is provided by email and in-product channels during our normal business operations and on a commercially reasonable basis for the applicable plan.

If Customer terminates or elects not to renew, we will provide standard offboarding support and export capabilities as described in the Agreement, including continued access to the standard export package during the offboarding period, reasonable remote coordination for handover of completed standard export artefacts, and reasonable responses to transition-related questions about the standard export structure.

Implementation work, data migration, transformation, validation, custom integrations, custom reporting, customer-specific remediation work, regulator questionnaires, expanded security reviews, consulting, enhanced transition assistance, and other non-standard or project-based services are outside standard subscription and support scope unless expressly included in the applicable plan, SLA, or Order Form. Where we agree to perform such work, it may be provided at our then-current rates under a written change order, Order Form update, statement of work, or similar instrument describing scope, assumptions, timing, dependencies, and fees, and we are not required to begin until the parties agree that instrument. Out-of-scope requests, changes in assumptions, or Customer-caused delays may change pricing, timelines, sequencing, staffing, and delivery commitments for the affected work. The parties may also agree in an Order Form or addendum on additional transition assistance, exit cooperation, recovery commitments, or resilience obligations, including for DORA or similar regulated outsourcing requirements.

Confidentiality

Confidential Information includes Account Data, business plans, pricing, security materials, technical documentation, and other non-public information designated as confidential or that a reasonable business person would understand to be confidential.

Each party receiving Confidential Information from the other party must:

- use it only for the purposes of the Agreement;
- protect it using reasonable technical, organisational, and contractual safeguards;
- disclose it only to personnel, contractors, professional advisers, and **Affiliates** (entities that control, are controlled by, or are under common control with a party) who need to know it and are bound by appropriate confidentiality obligations.

Confidential Information does not include information that the receiving party can demonstrate:

- is or becomes public through no breach of the Agreement;
- was lawfully known to the receiving party without confidentiality restriction before disclosure;
- is lawfully received from a third party without confidentiality restriction;
- is independently developed without use of the disclosing party's Confidential Information.

If a receiving party is required by law, regulation, court order, or binding governmental request to disclose Confidential Information, it may do so only to the extent legally required and, where legally permitted, after giving the disclosing party prompt notice so the disclosing party may seek confidential treatment, a protective order, or other appropriate remedy.

These confidentiality obligations survive for 5 years after termination, except that Account Data and trade secrets remain protected for so long as they remain confidential under applicable law.

Intellectual Property

As between the parties, we retain all right, title, and interest in and to the Service, the Documentation, software, know-how, models, interfaces, and all related intellectual property rights, except for Account Data and Customer Organisation-owned materials.

If Customer provides feedback, suggestions, or improvement ideas, Customer grants us a non-exclusive, worldwide, perpetual, irrevocable, royalty-free right to use that feedback without restriction, provided we do not publicly identify Customer as the source without Customer's consent.

Warranties And Disclaimers

We warrant that we will provide the Service in a professional and workmanlike manner materially consistent with the Agreement.

During the applicable subscription term, the Service will materially conform to the Documentation in all material respects, subject to permitted changes under the Agreement.

We warrant that we have the right to provide the Service and to grant the rights expressly granted under the Agreement.

Except as expressly stated in the Agreement, the Service, Demo Accounts, Trials, Beta Features, and related materials are provided AS IS and AS AVAILABLE. We disclaim all implied warranties, including implied warranties of merchantability, fitness for a particular purpose, and non-infringement, to the maximum extent permitted by law.

Indemnities

We will defend Customer Organisation against a third-party claim alleging that the Service, when used by Customer Organisation in accordance with the Agreement, infringes that third party's intellectual property rights, and we will pay damages finally awarded or amounts agreed in settlement, subject to the Higher Cap described under Liability And Insurance. In addition, we may at our option: (A) procure the right for Customer Organisation to continue using the Service; (B) modify or replace the Service to avoid infringement without material degradation in functionality; or (C) if neither (A) nor (B) is commercially practicable, terminate the affected Order Form or Subscription and refund the pro rata fees for the unused portion of the term. These are our sole and exclusive additional obligations for such a claim. This obligation does not apply to claims arising from Account Data, Customer Organisation modifications, combinations not supplied by us, or use of the Service outside the Agreement.

Customer Organisation will defend us against third-party claims to the extent caused by Customer Organisation's unlawful use of the Service, Customer Organisation's submission of Account Data or other materials without the necessary rights, or Customer Organisation's instructions or content that infringe applicable law or third-party rights, and will pay damages finally awarded or amounts agreed in settlement by Customer Organisation.

The party seeking indemnification must promptly notify the indemnifying party of the claim, provide reasonable cooperation, and allow the indemnifying party to control the defence and settlement, except that no settlement admitting fault or imposing ongoing obligations on the indemnified party may be entered without that party's prior written consent, not to be unreasonably withheld.

Liability And Insurance

Nothing in the Agreement excludes or limits liability for:

- fraud or fraudulent misrepresentation;
- willful misconduct;
- liabilities that cannot be excluded or limited under applicable law;
- payment obligations (fees owed under the Agreement remain uncapped).

Subject to the paragraph above:

Cap basis. For the purposes of this section, "fees" means amounts paid or payable by Customer under the Agreement, excluding taxes, pass-through costs, and third-party charges. Unless an Order Form states otherwise, each cap in this section is the aggregate limit for all claims arising out of or in connection with the Agreement, measured by the fees paid or payable by Customer in the 12 months immediately preceding the event giving rise to the first claim for which the relevant cap is invoked. Each cap includes any costs and expenses, including reasonable attorneys' fees.

General Cap. Except as stated below, each party's aggregate liability arising out of or in connection with the Agreement is limited to the fees paid or payable by Customer in the 12-month period (the **General Cap**), unless an Order Form states a different cap.

Higher Cap. For breach of confidentiality, indemnification obligations under the Agreement, infringement or misappropriation of the other party's intellectual property rights, and a party's violation of applicable data protection law or failure to implement the security, privacy, breach-notification, or processor obligations expressly required by the Agreement, each party's aggregate liability is limited to **4x** the fees paid or payable by Customer in the 12-month period (the **Higher Cap**). An Order Form may state a different cap, and where applicable law requires a higher or uncapped liability standard, that standard applies instead.

For Free Tier, Demo-only, Trial, or other no-fee use, both the General Cap and the Higher Cap are zero.

For clarity, unauthorised access to, disclosure of, loss of, or inability to restore Account Data, and any associated privacy, security, breach-notification, or processor-obligation failures, are treated as data protection / security matters for cap purposes and fall within the Higher Cap unless applicable

law requires otherwise.

For clarity, contractual duties to notify, cooperate, and assist in relation to incidents, personal data breaches, operational resilience events, or regulatory matters do not by themselves create uncapped damages exposure unless such uncapped exposure is required by applicable law.

Separately from the caps above, neither party is liable for indirect, incidental, special, punitive, or consequential damages, or for loss of profits, revenue, goodwill, business opportunity, or anticipated savings, even if advised of the possibility of such damages.

Insurance. We maintain commercially reasonable professional liability (errors and omissions) and general liability insurance appropriate for a B2B SaaS provider of our size and risk profile. On reasonable request, we will provide a certificate of insurance or other evidence of coverage. If Customer requires higher minimum limits or additional coverage types, the parties may agree those requirements in an Order Form, in which case we will maintain the agreed coverage during the applicable subscription term, subject to any express limitations stated in the Order Form and to any premium adjustment or commercial concession the parties agree.

Suspension And Termination

We may suspend or restrict access where reasonably necessary to prevent security harm, investigate abuse, respond to legal requirements, or enforce these Terms. We may suspend or terminate access if Customer materially breaches the Agreement, fails to pay undisputed fees, creates security risk, or uses the Service unlawfully or abusively.

Either party may terminate the Agreement for material breach if the other party does not cure that breach within 30 days after written notice. A payment breach may be cured within 10 days, as set out under Non-payment below. A breach that cannot reasonably be cured may be terminated immediately. A breach notice must describe the issue in reasonable detail so that the receiving party can respond and cure it.

Non-payment. If an undisputed invoice remains unpaid after the due date, we may issue notice of non-payment and require cure within 10 days. During that 10-day cure period we may place the Service in read-only mode or otherwise limit functionality. Wherever access is temporarily restricted for non-payment, whether during the cure period or after a subsequent suspension, we will use commercially reasonable efforts to preserve machine-readable export capability for up to 30 days from the date access is first restricted, unless doing so would create a security or legal risk.

Completed export artefacts may remain available for secure re-download during that period, subject to retention settings, authentication, and any applicable legal or security constraints. If the overdue amounts remain unresolved after that 10-day cure period, we may suspend access and, if the breach continues, terminate the affected Service or the Agreement. Termination for non-payment does not shorten the post-termination export period described under Your Data; the 30-day period in this paragraph is the minimum export capability preserved while access is restricted, not a substitute for that period.

Nothing in this section prevents a party from taking action reasonably necessary to address an immediate security threat, abuse, legal-compliance obligation, or operational-resilience risk during an otherwise applicable cure period.

Either party may also terminate the Agreement immediately by written notice if the other becomes insolvent, enters liquidation, suspends payment of its debts, has a receiver, administrator, trustee, or similar officer appointed over all or a substantial part of its assets or business, or becomes subject to a comparable insolvency or bankruptcy proceeding, except to the extent restricted by applicable law, including any applicable moratorium, suspension-of-payments protection, or court-approved restructuring restriction under Dutch insolvency law.

Customer may also terminate the affected Service by written notice if we suffer a prolonged service failure, security failure, or material operational resilience failure that materially defeats the purpose of the Service for Customer, and we do not restore or remediate the affected Service within a commercially reasonable period after notice, taking into account the severity of the issue and any agreed service commitments.

Customer may terminate the Agreement by cancelling all applicable Subscriptions or by written notice effective at the end of the then-current Commitment Term, unless the Commercial Terms expressly provide an earlier termination right. Customer's right to terminate an individual Subscription for convenience, and the notice required to prevent automatic renewal, are set out under Subscription Term, Renewal, And Changes To The Service. Termination or expiration does not relieve Customer of payment obligations accrued before the effective termination date.

General

Export controls, sanctions, and anti-bribery. Customer will not use the Service in violation of applicable export control, sanctions, anti-corruption, or anti-bribery laws. Each party will comply with applicable anti-bribery and anti-corruption laws in connection with the Agreement.

Assignment and change of control. Neither party may assign the Agreement without the other party's prior written consent, except that either party may assign without consent to an Affiliate or in connection with a merger, acquisition, corporate reorganisation, or sale of substantially all of its relevant assets, provided the assignee assumes the assigning party's obligations.

Publicity. We may identify Customer as a customer of the Service, and use Customer's name and logo in customer lists, on the firmfact website, and in similar promotional materials, only where Customer has given prior written consent through a documented in-product consent control, an Order Form provision, or written confirmation by an authorised Customer representative. Customer may withdraw consent at any time through the in-product control or on reasonable prior written notice, after which we will cease new use within a reasonable period, except for materials already in circulation that cannot reasonably be recalled.

Force majeure. Neither party is liable for delay or failure to perform caused by events beyond its reasonable control, excluding payment obligations.

Notices. Formal notices must be sent to the receiving party's designated notice email or physical address, unless an Order Form provides a different mechanism. Notices to Dutchcode B.V. trading as Firmfact must be sent to legal@firmfact.com with a copy to the physical address listed below. Non-renewal and convenience-termination notices may also be submitted through the designated in-product billing workflow where it is available for the relevant Subscription. A notice is effective when received through one of those permitted channels.

Changes to these Terms. The following paragraph applies to changes to these Terms. Changes to the Service are governed by Subscription Term, Renewal, And Changes To The Service.

We may update the Terms and Conditions from time to time. For a paid subscription, the version accepted at the start of the then-current subscription term will remain in effect during that term, except for changes required by law or changes that do not materially reduce Customer's rights or increase Customer's obligations. We will provide at least 30 days' prior notice by email and/or in-product notice for material adverse changes, and any such change will apply no earlier than renewal unless Customer expressly agrees earlier. Non-material changes may be posted with an updated effective date.

Severability and waiver. If any provision of the Agreement is held unenforceable, the remaining provisions remain in effect to the fullest extent permitted by law. A failure or delay in exercising a right under the Agreement does not waive that right.

Governing law and jurisdiction. The Agreement is governed by the laws of the Netherlands, excluding its conflict-of-laws rules. The competent courts of 's-Hertogenbosch, the Netherlands have exclusive jurisdiction over disputes arising out of or in connection with the Agreement, unless applicable law requires otherwise.

Survival. The following provisions survive termination or expiration of the Agreement: payment obligations accrued before termination, confidentiality, intellectual property, the Your Data section, the Acceptable Use section, the AI Features And Processing Boundaries section, warranty disclaimers, liability limits, retention and deletion obligations, order of precedence, governing law and jurisdiction, and any other provisions that by their nature should survive.

For clarity, our commitment not to use Account Data, including de-identified or aggregated derivatives, to train, fine-tune, or improve any machine-learning or AI model continues to apply after termination or expiration, for as long as we hold any Account Data, including while Account Data remains in backups pending expiry of the applicable retention cycle.

Defined Terms

- **Account** means a tenant-scoped instance of the Service associated with a Customer Organisation, including its Account Data, settings, users, usage records, billing scope, and service scope.
- **Account Data** means data, files, documents, records, prompts, configurations, and other content submitted to or processed through the Service for a specific Account on Customer Organisation's behalf.
- **Agreement** means the contract package between Customer and Dutchcode B.V. trading as Firmfact described in the These Terms And The Rest Of The Agreement section.
- **Commercial Terms** means the commercial selections recorded for a Subscription (plan selection, pricing, Commitment Term, billing cadence, invoice timing, payment term, discount, tax treatment, first invoice date, usage entitlements, and SLA eligibility), as recorded in an accepted in-product workflow, together with any additional commercial selection recorded in a Subscription Agreement or an Order Form.
- **Commitment Term** means the committed subscription period selected for a Subscription and recorded in the Commercial Terms, for example monthly, quarterly, one year, or multi-year, measured independently of the invoice cadence.

• **Customer**, also referred to in these Terms as **Customer Organisation**, means the legal entity that enters into the Agreement. The two terms have the same meaning.

• **Documentation** means user guides, implementation materials, and technical information that we make available for the Service.

• **DPA** means the Data Processing Agreement that forms part of the Agreement whenever Dutchcode B.V. trading as Firmfact acts as processor for Account Data containing personal data.

• **Enterprise Plan** means a Paid Plan marketed as Enterprise, with the entitlements recorded in the Commercial Terms.

• **Enterprise Services** means the enterprise assurance and regulated-outsourcing commitments identified as such in the Security, Operational Resilience, And DORA section: the scoped audit or control review, the operational-resilience and regulated-outsourcing cooperation baseline, and any related enterprise-only commitments expressly stated in an Order Form.

• **Order Form** means a written order or similar commercial ordering document between the parties.

• **Paid Plan** means any non-free plan for the Service.

• **Professional Plan** means a Paid Plan marketed as Professional, with the entitlements recorded in the Commercial Terms.

• **Service** means the firmfact platform, APIs, support channels, and related hosted services that we make available to Customer.

• **SLA** means the Service Level Agreement, which applies only where the Commercial Terms expressly state that the applicable Subscription is SLA-eligible.

• **Subscription** means the commercial plan, billing settings, usage entitlements, and applicable service commitments for a specific Account, as recorded in the Commercial Terms.

• **Subscription Agreement** means the in-product or written subscription agreement or order record used to capture plan selection, billing details, assent, and related evidence for a Paid Plan.

• **User** means an individual authorised by Customer to access the Service under a **User Account**, being the credentials and profile assigned to that individual.

Contact

Questions about these Terms may be sent to:

- legal@firmfact.com
- Dutchcode B.V., Litserstraat 20, 5275 BV Den Dungen, The Netherlands