firmfact

Privacy Notice

How firmfact Processes Personal Data

DOCUMENT CONTROL

VERSION
v2026-Q3

BUILD
2026-Q3.e0e12a6

PUBLISHED
30 September 2026

CLASSIFICATION
Customer-Facing

DISTRIBUTION
Enterprise customers, prospects, auditors

© 2026 Dutchcode B.V.
Governed by Dutch law

Last updated: 30 September 2026

Overview

This is a B2B privacy notice. In many cases, your organisation decides how Account Data is used in the Service, while we process that data on your organisation's behalf. This Privacy Notice explains our controller-side processing and how privacy-related requests are handled. Where we process Customer-controlled Account Data on behalf of a Customer organisation, that processing is governed by the applicable Agreement and DPA.

We do not use customer Account Data to train, fine-tune, or improve any machine-learning or AI model. AI-assisted processing is part of how the Service works (document intake in particular uses automated extraction), and your content is processed only to provide, secure, support, and troubleshoot that functionality in accordance with the Agreement and DPA, as described in the AI Features And Processing Boundaries section below.

Who We Are

For the purposes described in this Privacy Notice, the provider of the Service is:

- **Dutchcode B.V. trading as Firmfact**
- Litserstraat 20, 5275 BV Den Dungen, The Netherlands
- privacy@firmfact.com

Our Role: Controller And Processor

We Act As Controller For

We act as **controller** for personal data we use for our own business operations, including:

- website operation;
- account registration and account administration;
- billing, invoicing, collections, and tax records;
- fraud prevention, abuse prevention, and security administration;
- sales, support, and contact handling, including walkthroughs booked through our website;
- registration for webinars and events we host;
- communications with prospects, customers, and authorised users;
- relationship management and contractual administration.

We Act As Processor For

We act as **processor** when Customer uses the Service to process personal data in Customer-controlled Accounts, including:

- uploaded files and attachments;
- user-entered business data;
- Account records created or maintained by Customer;
- contact records created within the Account;
- contract, invoice, allocation, and organisational data entered by Customer;
- personal data contained in customer documents or prompts processed through Service features.

When we act as processor, our processing is governed by the applicable Agreement and DPA.

Our processor role for Customer-controlled Account Data does **not** turn our own account administration, provider-side billing and collections, relationship management, or general support communications into processor activities. Those provider-side business operations remain controller-side activities under this Privacy Notice.

Differences in plan tier may affect commercial support or service commitments, but do not change the controller / processor role allocation described in this Privacy Notice.

Requests About Customer-Controlled Account Data

If you are an end user, employee, contractor, or contact whose data appears in a Customer-controlled Account, you should contact the relevant Customer organisation first. That organisation is usually best placed to respond to requests about access, correction, deletion, restriction, or portability of Account Data.

We will support our customers in responding to such requests where required under the DPA or applicable law.

Lawful Bases When We Act As Controller

When we act as controller, we rely on one or more of the following lawful bases under applicable data protection law, depending on the processing activity:

- **Contract performance** for account setup, service delivery, authentication, billing, subscription management, and support;
- **Legal obligation** for tax, accounting, statutory retention, sanctions, export-control, and regulatory recordkeeping;
- **Legitimate interests** for fraud prevention, abuse prevention, service security, operational monitoring, incident management, relationship management, walkthrough bookings and event registrations, and service analytics that still involves personal data, where those interests are not overridden by data-subject rights;
- **Consent** only where we specifically request it for a separate optional purpose and where it can be withdrawn.

Some of what we do never reaches this section at all. Where we reduce information to aggregate form so that it no longer identifies a customer or any individual and cannot reasonably be re-identified, it stops being personal data: no lawful basis is required for it and the bases above do not apply to it. The aggregate operational analytics described under How We Use Personal Data below is of that kind. Where analytics still involves personal data (tracing a fault through session and error records, for example), we rely on legitimate interests as set out above.

When Customer uses the Service to process personal data in Customer-controlled Accounts, Customer generally determines the purposes, means, and legal basis for that processing. In that context, we act as processor unless the parties expressly agree otherwise.

Categories Of Personal Data

Depending on how the Service is used, we may process the following categories of personal data:

- account and identity data, such as name, business email address, preferred language, and role information;
- authentication data, such as hashed passwords, login records, session identifiers, and SSO-related identifiers;
- billing and commercial data, such as legal entity name, billing contacts, invoice details, VAT or tax identifiers, and payment-related records;
- support and relationship data, such as support messages, chat records, requests, walkthrough bookings, event registrations, and communications with our team;
- operational and security data, such as IP address, device or browser metadata, system logs, incident records, sender-verification metadata, and security review events;
- Account Data, such as uploaded files, user-entered business records, contact information, and data contained in documents processed through the Service;
- AI feature inputs and outputs, including content processed by automated document extraction during ordinary use of the Service.

How We Use Personal Data

We use personal data to:

- provide, operate, secure, and support the Service;
- manage accounts, subscriptions, invoices, and contractual records;
- authenticate users and administer access controls, including SSO / OIDC-based sign-in where enabled for the selected plan or applicable Order Form;
- support customer-administered user lifecycle management, role assignment, and Account-scoped auditability within customer Accounts;
- detect, prevent, and investigate abuse, fraud, misuse, and security issues;
- communicate with customers and users about service operation, billing, legal updates, and support matters;
- arrange walkthroughs booked through our website and register people for our webinars and events, including sending the calendar invitation and video-call link;
- maintain service reliability, troubleshoot incidents, and improve performance;
- comply with legal, regulatory, tax, accounting, and audit obligations.

Where permitted by law, we may also use de-identified and aggregated data for non-AI internal service improvement, operational analytics, reliability, capacity planning, and security purposes, provided that the data does not identify a customer or any individual and cannot reasonably be re-identified. Because data in that form is no longer personal data, the lawful bases set out above do not apply to it; where information has not been reduced to that form, it remains personal data and one of those bases does apply. Such data is not used to train, fine-tune, or improve any machine-learning or AI model. We do not use such data to publicly identify or comparatively benchmark a customer without that customer's express written consent.

With a customer's prior written consent, we may identify that customer and use its organisation name and logo on our website, in customer lists, and in similar promotional materials. Consent given through the in-product customer reference control in Account settings (available only to account administrators), an applicable Order Form provision, or written confirmation by an authorised customer representative satisfies this requirement. The lawful basis for this processing is consent under Article 6(1)(a) GDPR; we process only the organisation name, logo, and related reference metadata necessary to display the reference. Consent can be withdrawn at any time through the same in-product control or on reasonable prior written notice; after withdrawal we cease new use within a reasonable period (typically within 30 days of confirmed withdrawal), except for materials already in circulation that cannot reasonably be recalled.

AI Features And Processing Boundaries

AI-assisted processing is part of how the Service works rather than a feature you switch on. Document intake in particular uses automated extraction, so files you upload are processed by our AI subprocessor in the ordinary course. Where Account Data is processed by AI-assisted functionality:

- we do **not** use Account Data, including de-identified or aggregated derivatives, to train, fine-tune, or improve any machine-learning or AI model, and we do not instruct or authorise any subprocessor or third party to do so;
- we process prompts, uploaded files, submitted content, and related outputs only to provide, secure, support, and troubleshoot the requested functionality in accordance with the Agreement and DPA;
- as between Customer and us, Customer retains its contractual rights in Account Data and Customer-specific outputs, subject to the Agreement; nothing in this Notice limits applicable data-subject rights;
- Customer remains responsible for reviewing outputs before using them for legal, compliance, operational, or business decisions.

EU AI Act posture. For AI-assisted functionality offered through the Service, firmfact 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 those applicable to general-purpose AI model providers, rest with the relevant upstream AI subprocessor. The Service is not designed to carry out, and is not used by firmfact to carry out, practices prohibited under Article 5 of the EU AI Act.

Cookies, Browser Storage, Monitoring, And Analytics

We do **not** use advertising cookies, marketing pixels, cross-site tracking, or behavioural profiling for marketing purposes.

We do use limited operational, reliability, and security monitoring that is necessary to run the Service responsibly.

This may include:

- essential session cookies and CSRF protection;
- temporary authentication and SSO state handling;
- browser-stored interface preferences such as theme or sidebar state;
- operational logging and error monitoring;
- edge and application security telemetry used to detect incidents and maintain platform reliability.

In a narrow factual sense:

- **Cloudflare** may process IP addresses and request metadata for traffic delivery, abuse prevention, caching, and edge security functions;
- **Sentry** may process diagnostic and security event data, including application errors and browser-reported policy violations, to help us detect and investigate operational and security issues.

These operational tools are not used for marketing, advertising, or cross-site behavioural analytics.

Public website analytics. On our public website only, and never within the authenticated application or for signed-in users, we use **Ahrefs Web Analytics** to understand aggregate visitor trends such as page views, referring sources, approximate country, and device or browser type. It is **cookieless** and privacy-preserving: it sets no cookies, does not track you across other websites, does not build advertising or behavioural profiles, and does not retain your IP address (an approximate location is derived from it, then the raw address is discarded rather than stored). Because it stores nothing on your device and no directly identifying data, it does not rely on cookie consent; where local law nonetheless requires notice or an opt-out for such technologies, we provide it.

Where consent is legally required for non-essential cookies or similar technologies, we will request it before activating those technologies. Essential security, session-management, and fraud-prevention technologies remain in use because they are necessary to operate the Service.

SSO And Identity Providers

When Customer enables **SSO / OIDC-based sign-in**, where available for the selected plan or applicable Order Form, authentication-related identifiers and sign-in metadata may be processed as described in this Notice.

This may include:

- user email address and display name received from the identity provider;
- provider identifiers and tenant or domain metadata;
- login timestamps, IP address, and session records;
- encrypted session or refresh tokens where needed for the configured flow.

Customer administrators are responsible for provisioning and deprovisioning users, assigning appropriate Account roles, and configuring their own identity provider and related access policies. Customer is also responsible for the availability and configuration of Customer's own identity provider. The identity provider's own privacy practices are governed by that provider and Customer's relationship with it.

Email-Based Ingestion And Sender Security

Where Customer enables email-based ingestion or submission workflows, we may process sender verification data, allow-list or block-list entries, routing metadata, message headers, and related security review events to protect customer Accounts, reduce abuse, and route inbound content correctly.

Each Account has its own intake address, and only senders an Account administrator has approved are eligible for automatic processing. Sender authenticity is checked with standard email authentication, and a message that fails those checks is not processed automatically, even from an approved sender.

These controls are used for operational security and abuse prevention. They do not by themselves expand the scope of Account Data exported through ordinary Account export tools.

Data Sharing And Subprocessors

We may share personal data with subprocessors and service providers acting on our instructions and subject to contractual controls, including providers used for hosting, security, monitoring, email delivery, document or AI-related processing, billing, and related operational functions. Depending on the context, these recipients may act as our processors, our sub-processors when we act on behalf of a Customer, our own controller-side operational vendors, or independent recipients where disclosure is legally required.

Key controller-side and operational vendors currently include:

- **Cloudflare Ireland Ltd.** for traffic delivery, abuse prevention, caching, and edge security;
- **Sentry / Functional Software, Inc.** for diagnostic, monitoring, and security-event handling;
- **Ahrefs Pte. Ltd.** for cookieless, aggregate visitor analytics on our public website only (not applied to the authenticated application or to signed-in users);
- **Google** (Google Workspace) for business email, and for the Google Calendar invitations and Google Meet links we send for walkthroughs, webinars, and events;
- **Lettermint** for transactional email delivery;
- **Moneybird B.V.** (Zwolle, The Netherlands) for invoicing and billing administration under our Dutch statutory accounting obligations; and
- any additional payment provider used for the relevant subscription workflow, identified in the sub-processors register where applicable.

When we process Customer Personal Data on behalf of a Customer, we use the following **processor-side subprocessors** (current as of the date of this Notice):

- **Hetzner Online GmbH** (Germany): primary hosting, databases, object storage, and backups for Account Data;
- **Cloudflare Ireland Ltd.** (Ireland / EU points of presence): DDoS protection, web application firewall, TLS termination, and email routing for the Service;
- **Lettermint** (Netherlands): transactional email delivery for Service notifications and account workflows;
- **Sentry / Functional Software, Inc.** (USA; EU data residency region: Frankfurt): application error monitoring and performance diagnostics; international transfers safeguarded by the EU-US Data Privacy Framework and Standard Contractual Clauses where required; and
- **Mistral AI SAS** (Paris, France): AI inference for the AI-assisted parts of the Service, including the automated document extraction that runs when files are uploaded. Inference requests are sent to the provider's EU regional endpoint, which serves them from EU/EFTA data centres. Mistral processes Customer Personal Data under our documented instructions. We do not instruct or authorise Mistral to use that data for model training, fine-tuning, or improvement, and the provider-side training setting is disabled in our organisation account. Zero data retention is also enabled for that account, so Mistral does not retain inference content, meaning our requests and its responses, once a request has been processed.

Some providers listed above may appear in both controller-side and processor-side contexts depending on whether we process data for our own operations or strictly on Customer's instructions. Roles, data categories, and regions for processor-side recipients are also set out in the applicable DPA.

A detailed processor-side subprocessor register (CSV) is available from the Security Documents area in Customer's account after onboarding, and on request for enterprise diligence. That register is the authoritative machine-readable list when field-level detail is required.

We may also disclose personal data:

- where required by law, regulation, court order, or binding governmental request;
- in connection with a merger, acquisition, financing, reorganisation, or sale of business assets;
- where necessary to protect rights, investigate misuse, or respond to security incidents.

We do not sell personal data.

Development tools used for source control, CI/CD, and issue tracking are kept outside ordinary customer personal data flows. In particular, customer personal data is not intentionally sent to such development systems.

Data Residency And International Transfers

Primary production infrastructure and Customer-controlled Account Data hosting are based in Hetzner data centres in Germany, with specific functional processing performed primarily by EU-based subprocessors listed in the DPA and processor-side subprocessor register. The controller-side and operational vendors identified in this Privacy Notice are maintained separately from that processor-side register because their role depends on the context of the processing. Current vendor details, roles, and regions may also be provided through our enterprise diligence materials on request.

If personal data is transferred outside the EU / EEA, we will implement the safeguards required by applicable law, such as the European Commission's Standard Contractual Clauses together with any supplementary measures that are reasonably required.

Retention, Export, And Deletion

We retain personal data for as long as reasonably necessary to provide the Service and fulfil the purposes described in this Privacy Notice, subject to legal, contractual, and operational retention requirements.

Deleting a user profile, removing Account access, or disabling a user account does not necessarily delete controller-side billing, account-administration, support, security, tax, audit, or legal-retention records. Those records may continue to be retained for the periods described below where required for contract administration, dispute resolution, legal compliance, security, or defence of claims.

We retain provider-side operational records only for as long as needed for the purposes described in this Notice, including security, support, billing, compliance, and service administration.

As a general guide:

- support and account-administration records may be retained for up to 24 months after account closure;
- operational security logs are retained for defined, limited periods by log type (authentication events: 180 days; API/MCP access logs: 365 days; other security logs: up to 180 days), unless a longer period is required for a documented security investigation, legal hold, or compliance obligation;
- Customer Personal Data processed on behalf of a customer is returned or deleted under the Agreement and DPA, subject to backup rotation, legal retention obligations, and narrowly scoped retained records. Deletion of an Account additionally destroys that Account's document-encryption key, with the result that files stored under it become permanently unreadable rather than merely marked as deleted. This is cryptographic erasure in the sense of NIST SP 800-88.

Some categories of data, such as configurable chat or inbox retention content, may be retained according to the settings made available in the Service.

If backup data is restored for disaster recovery, integrity verification, or security remediation, the restored data remains subject to the same access restrictions and is re-deleted or allowed to age out under the applicable backup retention cycle once the restoration purpose is complete.

Deletion and retention exceptions under this Privacy Notice are intended to align with the Terms and the DPA.

Where we process personal data on behalf of a customer, the applicable data-processing terms are governed by the DPA and not by plan tier, except to the extent a specific feature is not enabled for the relevant Subscription.

Data Portability And Access

Customer administrators may use the export tools made available in the Service to obtain a machine-readable Account export of Customer-controlled Account Data, subject to documented technical and operational limits. The standard export package includes a current-state snapshot of Account Data, the Account Audit Trail for the selected export scope, referenced files, and manifest/checksum metadata, using the standard formats made available by the Service for the relevant data type,

including CSV and JSON where supported.

Standard export tools are not designed to export every internal provider-side record. Provider-side security logs, abuse-prevention records, infrastructure telemetry, and similar internal security materials may be retained separately and are not part of the standard customer export package unless expressly stated otherwise in an Order Form.

Where service access is temporarily restricted for billing reasons, we use commercially reasonable efforts to preserve export capability for up to 30 days, unless doing so would create a security or legal risk. Completed export artefacts may remain available for secure authenticated re-download during that period subject to retention settings and any applicable legal or security constraints. We provide standard offboarding support including continued access to the export package during the applicable offboarding period and reasonable remote coordination for handover of completed export artefacts. More specific export or offboarding commitments in an Order Form or the DPA will prevail where applicable.

Security

We use commercially reasonable technical and organisational safeguards appropriate to the nature of the Service and our risk profile, including measures relating to encryption in transit and at rest, access management, separation of Customer Accounts, backups, application-level logging, error monitoring and alerting, vulnerability management, and incident response.

Encryption of stored data protects data held on media at rest, including decommissioned, copied, lost, or seized hardware. It does not by itself protect against the misuse of validly issued credentials or against a compromise of the running Service, where data is available to the Service in the ordinary course; those risks are addressed by access management, Account separation, logging, and incident response.

A public summary of our security posture, including hosting, authentication, encryption properties, Account separation, and how to report a vulnerability, is published at firmfact.com/security. Further technical and organisational detail is available through our customer diligence materials and the DPA.

No method of transmission or storage is completely secure, but we work to reduce risk and respond appropriately to incidents.

Personal Data Breaches

Where we act as controller, we will handle personal data breaches in accordance with applicable law.

Where we act as processor for Customer-controlled Account Data, we will notify Customer without undue delay after becoming aware of a personal data breach affecting Account Data and provide the information and cooperation required under the DPA and applicable law.

Children And Minors

The Service is designed for business users and is not directed to children. We do not knowingly collect personal data directly from children in a consumer context. If you believe personal data has been submitted to us inappropriately, contact us using the details below.

Your Rights

Depending on applicable law and our role in the processing, you may have rights including:

- access;
- rectification;
- erasure;
- restriction;
- objection;
- portability;
- withdrawal of consent, where processing is based on consent;
- complaint to a supervisory authority.

Your rights may vary depending on whether we act as controller or processor for the relevant data. We do not make solely automated decisions with legal or similarly significant effects about you.

If we act as controller for the relevant data, you may contact us directly using the details below.

If the request relates to Customer-controlled Account Data, please contact the relevant Customer organisation first.

If you are in the Netherlands, you may also lodge a complaint with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens). If you are located elsewhere, you may lodge a complaint with the supervisory authority in your usual place of residence, work, or the place of the alleged infringement, where applicable.

Changes To This Privacy Notice

We may update the Privacy Notice 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.

Contact

For privacy questions or requests:

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