Firmfact

Data Processing Agreement

GDPR-Compliant Processing of Customer Personal Data

DOCUMENT CONTROL

VERSION
v2026-Q1

PUBLISHED
April 10, 2026

CLASSIFICATION
Confidential

DISTRIBUTION
Enterprise customers, prospects, auditors

© 2026 Dutchcode B.V.
Governed by Dutch law

Between Customer (Controller) and Dutchcode B.V. trading as Firmfact (Processor)

This Data Processing Agreement ("DPA") forms part of the Agreement between Customer ("Controller") and Dutchcode B.V. trading as Firmfact ("Processor") for the provision of the Firmfact services.

This DPA applies automatically whenever Customer uses the Service to process personal data for which Dutchcode B.V. acts as processor, regardless of plan tier. It sets out the parties' rights and obligations under Regulation (EU) 2016/679 ("GDPR") and other applicable data protection laws. The Controller remains responsible for determining the purposes, means, and lawful basis of processing to the extent required by applicable law, including decisions about user lifecycle, role assignment, and customer-managed identity configuration.

Article 1: definitions

Personal Data: Any information relating to an identified or identifiable natural person as defined in Article 4(1) GDPR.

Controller: Customer, being the natural or legal person which determines the purposes and means of processing Personal Data.

Processor: Dutchcode B.V. trading as Firmfact, processing Personal Data on behalf of the Controller.

Data Subject: The identified or identifiable natural person to whom Personal Data relates.

Processing: Any operation performed on Personal Data as defined in Article 4(2) GDPR.

Sub-processor: Any processor engaged by Firmfact to process Personal Data on behalf of the Data Controller.

Services: The market data cost and contract management platform and related services provided by Firmfact.

Article 2: scope and purpose of processing

2.1 **Scope:** This DPA applies to all processing of Personal Data by the Processor in connection with the provision of the Services to the Controller.

2.1A **Plan Neutrality:** This DPA applies regardless of plan tier and is not reduced or limited by SLA eligibility, support tier, or commercial plan selection, except to the extent a specific processing feature is not enabled for the relevant Subscription.

2.2 **Documented Instructions:** The Processor will process Personal Data only on documented instructions from the Controller, including as set out in the Agreement, this DPA, and the Controller's use and configuration of the Service. If the Processor believes an instruction infringes applicable data protection law, it will inform the Controller without undue delay.

2.3 **Purpose:** Personal Data will be processed only as necessary to provide, secure, support, and operate the Services in accordance with the Controller's documented instructions. This may include the following activities:

- Provision of the Firmfact platform and services for Customer-controlled Accounts
- User authentication and Account access management
- SSO / OIDC-based sign-in, where configured for the relevant Subscription
- Role-based user provisioning, deprovisioning, and Account access control based on Controller configuration
- Customer-requested support limited to Account incidents, diagnostics, and Account Data made available by the Controller
- System monitoring and security for Customer-controlled Account Data
- Email-based ingestion security controls, including sender verification and routing review where enabled by the Controller
- Backups, resilience, and recovery operations for Customer-controlled Account Data
- Compliance with legal obligations that apply to the Processor in relation to Customer Personal Data

For clarity, provider-side account administration, Marketdata.ai billing and collections, relationship management, and general support communications are controller-side activities described in the Privacy Notice and are not processor activities under this DPA.

2.4 Confidentiality Of Personnel

The Processor ensures that persons authorized to process Personal Data are subject to appropriate confidentiality obligations, whether by contract, policy, or law. The Controller remains responsible for determining which customer administrators and users should receive access, which roles they should hold, and whether the configured access model is appropriate for the Controller's own internal controls.

Article 3: categories of data and data subjects

3.1 Categories of Data Subjects

- Employees and contractors of the Data Controller
- Authorized users of the Firmfact platform
- Contact persons at vendor and client organizations

3.2 Categories of Personal Data

- Identity data (name, employee ID, job title)
- Contact data (email address, phone number)
- User Account data (username, encrypted password, preferences)
- Account usage data (login timestamps, feature usage, IP addresses associated with Account access, role assignments, and access-scope records)
- Support materials and diagnostics made available by the Controller for Account troubleshooting
- Business data (organizational structure, cost centre assignments)
- Document data (uploaded files, extracted text, metadata)
- Financial data (invoice details, contract terms, pricing information)
- Sender verification and email-routing metadata for customer-enabled inbound ingestion workflows

3.3 SSO Authentication Data

When SSO / OIDC-based sign-in is configured for the relevant Subscription, the following data is processed:

- Identity Provider identifiers and session tokens
- Refresh tokens (encrypted at rest using AES-256)
- IdP-provided user attributes (email, name, profile)
- SSO login timestamps and IP addresses
- Domain verification records for allowed domains

3.4 Document Processing Details

Personal Data within uploaded documents may include:

- Names and signatures on contracts and invoices
- Email addresses in document headers and correspondence
- Contact information of vendor representatives
- Employee identifiers in cost allocation documents
- Financial transaction details involving individuals

Article 4: technical and organizational measures

4.1 Firmfact implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including:

- Encryption of Personal Data at rest using AES-256 encryption
- Encryption of Personal Data in transit using TLS 1.2 minimum (TLS 1.3 where supported)
- Multi-factor authentication for administrative access
- Role-based access controls with least privilege principles
- Operational security monitoring, logging, and incident response procedures
- Automated vulnerability scanning and deployment security checks
- Continuous system monitoring and incident response procedures
- Secure backup and disaster recovery procedures
- Staff security training and access controls
- Physical security measures at data center facilities
- Data pseudonymization and anonymization where possible
- Uploaded documents retained according to the Data Retention Schedule in Appendix A; temporary processing artifacts are purged after extraction
- Purpose limitation for AI processing (no model training)
- Tenant isolation for document processing and storage

4.2 Document Processing Security

Additional measures for document processing include:

• SHA-256 checksums for duplicate detection and integrity verification

• Temporary processing in isolated containers

• Automatic purging of processing artifacts after completion

• AI-related processing is limited to providing the requested feature and not for training third-party or general-purpose AI models unless separately agreed in writing

• AI-assisted features are deployed in alignment with Regulation (EU) 2024/1689 ("EU AI Act"); the Service is not marketed for, and must not be used for, any prohibited practice under Article 5 of the EU AI Act, and Customer remains responsible for any high-risk use cases it may elect to pursue

• Any transient operational logging by AI subprocessors is limited to abuse prevention, service security, and troubleshooting and is not persistently retained for Customer profiling

• OCR and extraction results stored separately from source files

• Document access logging with customer-accessible account audit trail and internal event logging designed to support auditability

• Encrypted storage using AES-256 with platform-managed keys and tenant-scoped access controls

Article 5: sub-processors

5.1 **Authorization:** The Controller provides general written authorization for the Processor to engage Sub-processors for the processing of Personal Data, subject to the conditions set out in this Article.

5.2 Sub-processor Requirements

Firmfact ensures that any Sub-processor:

- Is bound by written contract imposing data protection obligations equivalent to this DPA
- Implements appropriate technical and organizational measures
- Supports EU/EEA-focused processing under the applicable contractual and technical controls
- Provides adequate guarantees regarding data protection compliance

5.3 Current Sub-processors

A current list of Sub-processors for Customer Personal Data is maintained in Firmfact's Sub-processor Register. Controller-side and operational vendors are maintained separately from that processor-side list.

- Hetzner Online GmbH (hosting and storage) - Germany
- Cloudflare Ireland Ltd. (CDN and security) - Ireland
- Lettermint (email services) - Netherlands (EU)
- Sentry/Functional Software GmbH (monitoring) - Germany
- Mistral AI SAS (AI processing, document analysis, OCR) - Paris, France

5.4 **Changes to Sub-processors:** The Processor will provide at least 30 days' prior notice before using a new Sub-processor in production for Customer Personal Data. The Controller may object on reasonable data protection grounds within that notice period.

5.5 **Objection Outcome:** If the Controller objects to a proposed new Sub-processor on reasonable data protection grounds, the parties will work in good faith to address the objection. If that cannot be done with commercially reasonable effort, the Processor may either refrain from using the proposed Sub-processor for the Controller's Personal Data or the Controller may terminate the affected Service before the change takes effect.

5.6 Development Systems Boundary

Development tools used for source control, CI/CD, and engineering issue tracking are outside the ordinary processing flow for Customer Personal Data. Firmfact does not intentionally send Customer Personal Data to GitHub, and GitHub is not a Sub-processor for Customer Personal Data under this DPA.

5.7 Customer Identity Providers

When SSO / OIDC is configured for the relevant Subscription, authentication data is exchanged with the Data Controller's Identity Provider (e.g., Okta, Azure AD, Google Workspace, Ping Identity). The Data Controller is responsible for its IdP's privacy and security practices, user lifecycle configuration, and availability. Firmfact does not act as a sub-processor for customer IdPs; rather, the IdP remains under the Data Controller's control.

Article 6: data subject rights

6.1 Assistance

Firmfact will assist the Data Controller in responding to Data Subject requests, including:

- Right of access (Article 15 GDPR)
- Right to rectification (Article 16 GDPR)
- Right to erasure (Article 17 GDPR)
- Right to restrict processing (Article 18 GDPR)
- Right to data portability (Article 20 GDPR)
- Right to object (Article 21 GDPR)

6.2 **Response Time:** Firmfact will provide assistance without undue delay and will ordinarily provide an initial substantive response within 3 business days after receiving a sufficiently detailed request from the Data Controller, taking into account the complexity of the request and the information reasonably available to the Processor.

6.3 **Additional Assistance:** The Processor will provide reasonable assistance to the Controller with security assessments, data protection impact assessments, and prior consultations with supervisory authorities where required under Articles 35 and 36 GDPR, taking into account the nature of processing and the information available to the Processor.

6.4 **Data Export:** The Controller may export Personal Data in machine-readable format through the platform's export functionality, including current-state Account Data snapshot data, the Account Audit Trail for the selected export scope, referenced files, and manifest/checksum metadata appropriate to the selected export scope, subject to documented technical and operational limits and any agreed offboarding procedures. Standard export tools do not include every provider-side record; internal security logs, abuse-prevention records, and similar internal materials remain outside the standard export package unless expressly stated otherwise in a binding commercial document.

Article 7: international transfers

7.1 **Primary Hosting:** Primary production infrastructure is hosted in Hetzner data centres in Germany, with specific functional processing currently performed primarily by EU-based subprocessors listed in the subprocessor register.

7.2 **International Transfers:** The Processor will not transfer Customer Personal Data outside the EEA, the United Kingdom, or Switzerland unless it has implemented a valid transfer mechanism under applicable data protection law for that transfer. Where the transfer relies on the European Commission Standard Contractual Clauses, the applicable SCC module and the related annexes set out in Appendix B are incorporated into this DPA by reference.

7.3 **UK And Switzerland:** Where Customer Personal Data is subject to UK data protection law or Swiss data protection law, the applicable UK addendum or Swiss transfer language set out in Appendix B will apply to the same transfer to the extent required.

7.4 **Supplementary Measures:** The Processor will maintain and apply supplementary technical and organizational measures appropriate to the transfer risk profile, as described in Appendix B and Article 4.

7.5 **Transfer Information:** The Processor will provide the Controller, on request and subject to confidentiality and security restrictions, the current transfer appendix, the list of relevant transfer destinations, and a summary of the supplementary measures used for applicable transfers.

Article 8: personal data breaches

8.1 **Notification:** The Processor will notify the Controller's designated privacy, security, or legal contact without undue delay after becoming aware of a Personal Data breach affecting Customer Personal Data and will aim to provide the initial notification within 24 hours where reasonably practicable.

8.2 Information to be Provided

The notification will include:

- Description of the nature of the breach
- Categories and approximate number of Data Subjects affected
- Categories and approximate number of Personal Data records affected
- Likely consequences of the breach
- Measures taken or proposed to address the breach

8.3 **Assistance:** Firmfact will provide all reasonable assistance to enable the Data Controller to meet its breach notification obligations under Articles 33 and 34 GDPR.

Article 9: audits and inspections

9.1 **Audit Rights:** The Controller may audit the Processor's compliance with this DPA and applicable data protection law on reasonable prior notice.

9.2 Audit Process

Audits may be conducted:

- No more than once per year unless required by law or a reasonably suspected material breach justifies an additional audit
- Using documentation, questionnaires, remote evidence, and virtual meetings first where reasonably sufficient
- On-site inspections coordinated in good faith under reasonable confidentiality, security, and scheduling requirements
- At the Controller's expense, unless the audit reveals a material breach of this DPA by the Processor, in which case the Processor bears the reasonable audit costs

9.3 **Information Rights:** The Processor will make available information reasonably necessary to demonstrate compliance with this DPA, subject to confidentiality, privilege, security, and protection of other customers' information.

9.4 **Commercial Assurance Separation:** Commercial assurance, diligence support, and scoped control-review rights under the Agreement are separate from the audit, information, and assistance rights set out in this DPA. Those DPA rights apply independently of plan tier.

Article 10: termination and data return

10.1 Data Return

Upon termination of the Services, Firmfact will:

- Provide the Data Controller with access to export Personal Data made available through the Service's export functionality in a machine-readable format
- Delete or return Personal Data within 180 days after termination or expiration of the Services, unless applicable law requires retention or the parties agree on a different offboarding period
- Provide written confirmation of the completion of the standard deletion workflow upon request
- Ensure Sub-processors comply with the same deletion requirements

10.2 **Legal Retention:** As detailed in Appendix A, Firmfact retains limited account metadata (up to 24 months for reactivation and dispute resolution), Account Audit Trail records and related standard export artifacts where required by law or contract, internal security logs where required for legal, security, or compliance purposes, and database backups (Hetzner server snapshots: 7-day rolling; WAL-G archives: 35-day rolling). All retained data remains subject to continued confidentiality and data protection obligations under this DPA.

10.3 **Backup Restoration:** If backup data must be restored for disaster recovery, integrity verification, or security remediation, the restored data will remain access-restricted and will be re-deleted or allowed to expire under the applicable backup retention cycle once the restoration purpose is complete.

Article 11: liability

11.1 **Mutual Responsibility:** Each party will be liable for its own compliance with applicable data protection laws.

11.2 **Liability Framework:** Except where this DPA expressly states otherwise for data protection matters, liability under this DPA is subject to the liability allocation and limitations set out in the Agreement.

11.3 **No Additional Uncapped Liability:** The notification, cooperation, and assistance duties in this DPA do not by themselves create uncapped damages exposure except to the extent such limitation is prohibited by applicable law.

Article 12: general provisions

12.1 **Duration:** This DPA remains in effect for the duration of the Services and any period during which Firmfact processes Personal Data on behalf of the Data Controller.

12.2 **Amendments:** For a paid subscription, the version of this DPA 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 Controller protections or increase Controller obligations. Material adverse changes will be notified at least 30 days in advance by email and/or in-product notice and, unless legally required sooner or expressly agreed earlier, will apply no earlier than renewal. Non-material changes may be posted with an updated effective date.

12.3 **Governing Law:** This DPA is governed by the laws of The Netherlands. Any disputes arising from or relating to this DPA shall be subject to the exclusive jurisdiction of the competent courts of 's-Hertogenbosch, Netherlands, in accordance with the Agreement.

12.4 **Conflicts:** In case of conflict between this DPA and the Agreement, this DPA prevails for data protection, privacy, data transfer, and processor-obligation matters.

12.4A **Uniform Processor Obligations:** Incident notification, subprocessor notice, assistance obligations, and international-transfer safeguards under this DPA, including Article 7 and Appendix B, apply without regard to plan tier.

12.5 **Contact:** For all data protection inquiries: privacy@firmfact.com. Security incidents and vulnerability reports may also be sent to security@firmfact.com.

12.6 **Compelled Disclosure:** If the Processor receives a binding request from a court, regulator, or other public authority requiring disclosure of Customer Personal Data, the Processor will, where legally permitted, promptly notify the Controller before disclosure and will disclose only the Personal Data legally required. The Processor may challenge, limit, or seek confidential treatment for the request where commercially reasonable and legally permitted.

Appendix a: record of processing activities (ropa)

In accordance with GDPR Article 30, this appendix documents the processing activities undertaken by Dutchcode B.V. trading as Firmfact (Processor) on behalf of Customer (Controller).

Processing Activity	Purpose	Categories of Data	Controller-Determined Legal Basis (if applicable)
Account User Access Management	Authentication and access control within Customer-controlled Accounts	Identity data, contact information, authentication credentials	Typically contract performance or another lawful basis determined by Controller
Document Processing	OCR & data extraction	Document-derived data	As determined by Controller in light of the relevant processing purpose
Account Audit Trail And Account Security Logging	Security, tenant isolation, and auditability of Customer Account activity	User actions, access logs, role changes, and security events tied to Customer-controlled Accounts	Typically legitimate interests, legal obligation, or another lawful basis determined by Controller
Cost Allocation	Financial analytics	User cost attribution	Typically contract performance or another lawful basis determined by Controller
Customer-Directed Support Investigations	Troubleshooting Account issues at the Controller's request	Support materials, chat excerpts, tickets, diagnostic exports, and relevant Account records shared by Controller	Typically contract performance or another lawful basis determined by Controller

This Appendix A covers processor-side handling of Customer-controlled Account Data. Provider-side account administration, Marketdata.ai billing and collections, relationship management, and general support communications are controller-side activities described in the Privacy Notice and are excluded from this processor appendix.

Data Retention Periods

- Service data: Duration of contract + up to 180 days (standard offboarding/export window)
- Chat conversations and inbound emails: User-configurable retention (1-999 days; 90-day default)
- Limited account/contact metadata: Up to 24 months after termination (e.g., reactivation, dispute resolution, and legal obligations)
- Customer-accessible audit trail records: Up to 7 years where required for compliance (SOX, regulatory requirements)
- Internal security logs: Retained for operational, security, and legal requirements under applicable retention schedules
- Database backups: Hetzner server snapshots (7-day rolling) + WAL-G archives (35-day rolling)
- Operational logs: 180 days

Data Recipients & Transfers

- Sub-processors: See Article 5 (Sub-processors) in this agreement
- International transfers are governed by Article 7 and Appendix B of this DPA
- Where a transfer outside the EEA, UK, or Switzerland occurs, the relevant transfer mechanism, transfer destination, and supplementary measures are identified in or supported by Appendix B and the applicable subprocessor register

Security Measures

- See Article 4 (Technical and Organizational Measures)
- Multi-tenant isolation with mandatory application-level scoping via ActsAsTenant
- Encryption at rest (AES-256) and in transit (TLS 1.2 minimum; TLS 1.3 where supported)
- Access controls with role-based permissions
- Event sourcing supports customer-accessible account audit trail records and internal event logging designed to support auditability

Appendix b: transfer mechanism annex

This Appendix B forms part of the DPA whenever Customer Personal Data is subject to a restricted international transfer. It documents the transfer mechanism, annex content, and supplementary measures applicable to that transfer.

B.1 Applicable Transfer Mechanism

- Module 2 (Controller to Processor) applies where Customer acts as controller and Dutchcode B.V. trading as Firmfact acts as processor
- For UK-restricted transfers, the UK International Data Transfer Addendum to the EU SCCs applies to the same transfer where required
- For Swiss-restricted transfers, the EU SCCs apply with the modifications required under Swiss data protection law where required

B.2 Annex I: Parties, Scope, And Transfer Details

- Data exporter: Customer, acting in the role identified by the applicable SCC module
- Data importer: Dutchcode B.V. trading as Firmfact, Litserstraat 20, 5275 BV Den Dungen, The Netherlands
- Categories of data subjects: employees and contractors of Customer, authorized users of the Service, and business contacts contained in Customer-controlled records
- Categories of personal data: identity data, contact data, account access and usage data, support materials, document contents, and related business records as described in Article 3 and Appendix A
- Frequency and duration: transfers occur on a continuous or ad hoc basis for the duration of the Services and any agreed offboarding period
- Purpose of processing: provision, support, security, resilience, and operation of the Service in accordance with the Agreement and documented instructions
- Transfer destinations and onward recipients are reflected in Article 5, the applicable subprocessor register, and the transfer records maintained under this Appendix B

B.3 Annex II: Technical And Organizational Measures

• The technical and organizational measures in Article 4 are incorporated into this Appendix B as Annex II

• Supplementary measures include encryption in transit and at rest, role-based access controls, tenant isolation, logging designed to support auditability, and documented incident response procedures

• Transfers are limited to what is necessary for the relevant Service function, and access to transferred data is restricted to authorized personnel and subprocessors with a need to know

B.4 Annex III: Sub-processors In The Transfer Chain

• Hetzner Online GmbH - hosting and storage - Germany

• Cloudflare Ireland Ltd. - CDN and security services - Ireland

• Lettermint - transactional email services - Netherlands

• Sentry / Functional Software GmbH - monitoring and diagnostics - Germany

• Mistral AI SAS - AI processing, document analysis, and OCR - Paris, France

• Any future sub-processor engaged for a restricted transfer will be added through the subprocessor notice process in Article 5 and reflected in the current subprocessor register

B.5 UK And Swiss Transfer Language

• For UK transfers, references to the competent supervisory authority and governing law will be read consistently with the UK addendum where required

• For Swiss transfers, references to the GDPR include the Swiss Federal Act on Data Protection where required, and data subjects in Switzerland may enforce rights in Switzerland to the extent required by applicable law

B.6 Transfer Documentation

• On reasonable request, the Processor will provide the current version of this Appendix B and information about the transfer destination relevant to Customer's restricted transfer

• Nothing in this Appendix B requires disclosure of information that would compromise security, privilege, or other customers' confidential information

This Data Processing Agreement (last updated April 10, 2026) constitutes a binding legal agreement between the parties.

Dutchcode B.V. | Litserstraat 20, 5275 BV Den Dungen, Nederland | VAT ID: NL865320202B01 | KVK: 90452151 | RSIN: 865320202