FTH Data Protection Specifications

Version 3.2, 27 September 2026. Supersedes version 3.1.

Provided by: Almustaqbal Alfadh for digital marketing Establishment (trading as FTH Digital Marketing)
CR 1009092617, Unified Establishment No. 7041553525, National Address RQFA2889
Concerning: FTH's Business Profile services (recovery of suspended Business Profiles, Business Profile restructuring and reporting, ongoing Business Profile management) and its FTH Maps platform product.

Prepared in line with the Saudi Personal Data Protection Law, its Implementing Regulations, and the SDAIA Regulation on Personal Data Transfer Outside the Kingdom.

0. This document and its governance

0.1 This document is a standalone public statement issued by Almustaqbal Alfadh for digital marketing Establishment ("FTH"), describing its personal data protection practices across all its services. It is not specific to any client and applies to every client whose data FTH processes.

0.2 The governing version of this document is the one published on the data protection page of FTH's website at https://fth.marketing/en/data-protection/ (Arabic: https://fth.marketing/data-protection/), dated and numbered, with a change log stating the date and scope of each amendment.

0.3 This document is updated by publication. FTH publishes each new or replacement sub-processor on its sub-processor register (section 6), and publication is the notice. FTH may engage a sub-processor from the date it is listed. A client may object on reasonable data protection grounds within thirty days of publication. FTH works with the client to address the objection, including by not using that sub-processor for the client's workspace where it supports an optional feature. Where the sub-processor is part of the platform's infrastructure and the objection cannot be resolved, the client may end the service that relies on it; this does not affect the client's other services with FTH. An objection does not suspend the engagement. Clarifications that reduce no existing commitment take effect on publication.

0.4 This document is issued in Arabic and English. The Arabic text prevails in case of any discrepancy.

0.5 Contracts refer to this document and do not amend it. Any additional commitment agreed with a client is recorded in that client's own contractual documents without reducing what is stated here.

1. Scope and services

1.1 FTH is a Saudi establishment registered under Commercial Registration No. 1009092617, based in Riyadh, Kingdom of Saudi Arabia.

1.2 FTH processes personal data as a processor under the Personal Data Protection Law and its regulations, on the documented instructions of the client as controller, unless the description of a specific service states otherwise.

1.3 FTH is a marketing agency with several departments. This document covers the part of its work that processes Business Profile data, which reaches clients in two forms.

Services, delivered by FTH's Business Profile department and presented at fth.sa:

a. Recovery of suspended Business Profiles.
b. Business Profile restructuring and reporting.

c. Ongoing Business Profile management.

Products, software FTH publishes under its own name at fth.marketing:

d. The FTH Maps platform, a software-as-a-service system for managing Business Profiles.

1.4 The platform is an independent product and not part of any service. A client may subscribe to the platform alone, take one of the services alone, or take a service and add the platform. Subscribing to one does not mean subscribing to any other, and the controls in this document apply to each as stated for it.

1.5 This document applies to personal data processed within these services, including platform user account data, the content of public reviews published on Business Profiles, and contact details appearing in them. FTH's public websites are outside its scope; their own privacy notices describe how they handle visitor data.

1.6 Reviews and profile performance data are retrieved only through Google's official APIs. For the platform, the client connects its own Google account directly to the platform. The platform has no other route to a client's profiles, and FTH's own accounts are not used to feed a client's workspace; this is enforced in the platform and tested. For the managed services, the client gives FTH's managed accounts access to its profiles on Google itself, and that access serves those services only. Each is a documented, revocable authorisation to process.

1.7 Processing of reviewer data relies on the controller's legitimate interest in managing public feedback about its own branches, applied to personal data the data subject has made public on Google. The controller remains responsible for its own legal basis assessment.

1.8 Platform user accounts: the name, work email, role, authentication data and action logs of the client's authorised users are processed to provide the service, enforce permissions and keep the audit trail.

1.9 Beyond the above, FTH collects no end-customer lists within these services, and no payment card data. Subscription payments are made through MyFatoorah: the buyer enters card details on MyFatoorah's own hosted payment page, which the platform links to, and no card data reaches FTH. The platform sends MyFatoorah the invoice amount and currency, the buyer's name and email address, and FTH's own internal payment reference. MyFatoorah is the trading name of Fatoorah for Electronic Marketing Company, a Saudi closed joint stock company (Commercial Registration 1010709742). FTH's digital payment services agreement with it was concluded on 16 September 2026, is governed by the laws of the Kingdom of Saudi Arabia, binds both parties to confidentiality during and after its term, and incorporates the provider's published terms and conditions. Identity and authorisation documents that a client provides for profile recovery are held in FTH Business Manager, each file encrypted, excluded from AI processing, and deleted with the client's other FTH Business Manager data (section 7).

1.10 FTH Business Manager is FTH's internal operations system. FTH personnel use it to deliver the Business Profile services; it is not offered to clients. It runs on the same infrastructure as the platform, within the European Union, and holds location data, service cases, documents and the contact details of the client's personnel. It holds no review data, and so no reviewer names or other reviewer identifiers. It exchanges Business Profile data with Google under FTH's own Google authorisation, limited to Google Business Profile and to profiles where the client has given FTH manager access. No data held in FTH Business Manager reaches FTH's dedicated Google Business Profile server or any model provider. FTH's internal business system, Odoo, runs on a server FTH administers itself, on infrastructure provided by Contabo GmbH within the European Union, and not on Odoo's hosted service. Odoo S.A. does not host it, and the installation's connections to Odoo S.A. services are disabled, so Odoo S.A. is not a sub-processor. FTH Business Manager reads only the latest invoice and payment status from Odoo and writes nothing to it.

2. Individuals' data

- A reviewer's publicly posted name is stored only if the client turns that option on for its workspace and records the accompanying acknowledgement of responsibility. The option is off by default. While it is off, the platform keeps no name, only the pseudonymous key described below, and new-review alerts name no one. While it is on, the name is not shown on any platform screen and is not included in any export: it appears only in new-review alerts sent to the client's own authorised users, and it is erased with the review. Turning the option off deletes the names already stored.
- Filtering and sorting work on review content and on the optional classification described below.
- No reviewer profiles are built. The platform holds a stable pseudonymous key per reviewer so that reviews by the same author can be linked. The key reveals no identity, is not shown to users, and is erased with the author's reviews.
- The platform neither collects nor infers any reviewer's gender. One optional classification exists. It is off unless the client deliberately grants a named member of its own staff the single capability that permits it; that capability belongs to no role. Where granted, that person may set an approximate gender by hand on an individual review. There is no dictionary, no model and no default, and nothing is recorded unless the client's staff choose to record it. The value is held apart from the review, is deleted with it, is not shown beside a reviewer's name, and is reported only as an aggregate in which any group of fewer than five is suppressed. The platform refuses a lower floor.
- That classification is also available only where the client has switched it on for the workspace. The switch is off everywhere until an administrator of the client turns it on, and turning it on requires a recorded acknowledgement of what is being asked for and by whom. FTH staff cannot turn it on for a client; they can only turn it off. Turning it off removes the ability to classify and leaves values already recorded in place, still deleted with their reviews, and the aggregate report then states that recording has stopped.
- AI analysis of review content is produced only as described in section 4, and only on the client's instruction.

3. Security controls, auditable against FTH's systems

- Isolation between clients is enforced by the database engine itself (forced row-level security) and proven by automated tests.
- Stored access credentials are encrypted (AES-256-GCM). Passwords are hashed with argon2id. All platform endpoints use TLS with strict certificate verification.
- When a platform user sets, changes or resets their own password, the platform checks it against Have I Been Pwned's list of passwords found in known data breaches. Only the first five characters of the password's hash are sent; the password, its full hash, email address, user identifier and workspace identifier are not sent. Requests to the service pass through Cloudflare's network. The check runs in the live service. Passwords that FTH sets for platform administrators through its operator tools are not checked. No contract is held with the service; its published terms apply.
- Audit trail: every privileged action is recorded in the same transaction as the action, and every displayed figure traces to the API call that produced it. Each export writes one audit entry (who, when, what, how many rows, for which period and which branches). Each retrieval of review data through the public API writes one audit entry (which key, which workspace, what was read and how many records). The key is identified on every call, its last use and rate window are kept, and failed attempts are throttled per network address. The audit trail also records the opening of a client workspace with platform authority, the

erasure confirmation entry, removal-request decisions and FTH personnel access. Individual page views inside the platform are not logged.

- Authentication events are kept in their own log for up to 90 days (section 7): sign-in and failed sign-in, the account where one exists or, where none does, a keyed one-way value in place of the address entered, the time, the network address and the method used. No password and no session token is recorded.
- Audit entries are append-only. They are edited or deleted in three cases only: clearing an erased review's content from the entries that recorded it (section 8); deletion at the end of a retention period in section 7; and redaction of personal data written into an entry by mistake.
- Permissions are set per capability for each user, and membership is checked again on every request.
- Two-factor authentication is available to all accounts, can be required per workspace at three levels, and is required for platform administrators (FTH accounts on the operator console).
- Support and operations access to a client workspace runs through named platform accounts with per-capability permissions. Opening a client workspace with platform authority writes an audit entry in the same transaction as the read. The read-only platform functions that do not write an audit entry form a closed list, enforced by automated tests.
- In the FTH Maps platform, FTH staff accounts cannot approve changes for the client, and client accounts cannot write to Google. The two authorities are separate.
- In the FTH Maps platform, nothing is written to the client's Google profiles without the client's approval. Every outbound change passes an approval step, and the approving user and time are recorded. In FTH's managed services, FTH writes to a client's profiles under that client's service agreement, and a review reply is posted only after an FTH person confirms it.
- Backups: the platform database is backed up every night. From the start of client services, the local copy is encrypted on the platform host and kept there for at least 14 days. The off-site copy is encrypted before it leaves the host and is held in Contabo object storage within the European Union as 7 daily, 4 weekly and 3 monthly snapshots.
- Restore tests: every night the newest local backup is restored into a separate test database and checked. The test passes only if every table's row count matches the count recorded in the backup and the row-level security policies are present. Where the live platform can be read, the restored database's counts of tables, security policies and applied database changes are compared with it. Each run records its date, the backup restored, the result and the row counts. Once a week the off-site copy is restored and checked in the same way, and its result is recorded.
- Retention: the platform's retention periods in section 7 are applied by an automated nightly job, except the rows section 7 describes as event-driven or kept for statutory reasons. FTH Business Manager deletion is carried out by FTH as a recorded action.
- External audit: no external audit statement has been issued for the platform as at this version. When one is issued, its scope, date and the auditor's statement will be added to this section.

4. AI processing

Each service is described on its own. Nothing in this section applies to a service it does not name.

Profile recovery, restructuring and management (FTH's managed services). FTH may use AI tools in analysing and managing Business Profiles, through its own paid subscriptions or paid API accounts with Anthropic, Google (Gemini) and OpenAI. Use of content for model training is turned off on every account. When FTH does so, business profile and review content reaches the provider as part of a conversation with a model there. The FTH Maps platform sends nothing to any model provider. FTH's dedicated Google Business

Profile server passes business profile and review content to a model provider only as a tool result, returned in response to an authenticated request from an authorised FTH staff member's AI assistant, which runs at that provider. FTH's rule is that its personnel use no other route. The protection applied to that content, and its limits, are set out at the end of this section. FTH does not rely on a data processing agreement with any of these providers for client personal data. The providers are listed in section 6.

AI features inside the FTH Maps platform. No feature of the platform sends review content, or any other client data, to a model provider, and AI is off by default. Any AI feature added later, including one that lets a client connect its own model provider key or buy model usage through FTH, stays off until an authorised user of the client switches it on for that workspace through an explicit consent step. Such a feature sends nothing to a model provider until an authorised user of the client has previewed the content to be sent and approved it. This document is updated and published under section 0 before any such feature can be switched on.

FTH personnel access during the managed services. Profile recovery, restructuring and management require FTH personnel to work inside the client's account, including inside the platform where the client uses it, to read profile and review data and to prepare periodic reports such as month-on-month comparisons and progress against agreed objectives. That access is limited to the personnel assigned to the client and is recorded in the audit trail. Content from that work reaches a model provider only by the route described above, under the rules at the end of this section.

FTH Business Manager. FTH Business Manager (1.10) holds no review data, and so no reviewer names or other reviewer identifiers. No data held in it reaches FTH's dedicated Google Business Profile server or any model provider.

Diagnostic data. FTH develops and improves the platform continuously. Where an authorised user of the client turns on diagnostic mode, or FTH turns it on to investigate a reported fault, the platform records technical detail about the fault, which may include client data present when it occurred. That data is used only to diagnose and fix the fault. Diagnostic capture is off on every workspace unless an authorised user of the client, or FTH investigating a fault the client reported, turns it on. It turns itself off after the capture window the workspace sets (seven days unless changed, and no more than thirty). Captured detail is kept for thirty days from capture and then deleted by the nightly retention job; turning capture off deletes every capture held for that workspace at once. Contact patterns are masked before storage, and credentials are not captured. The rules at the end of this section apply to captured data as to any other content. The software tools FTH uses to build and maintain the platform process no client data in the running service and are not sub-processors.

Rules for content that reaches a model provider.

- Where an AI feature of the platform is switched on, it runs on a provider key the client supplies. The client chooses that provider and plan, and the terms governing them are the client's own.
- FTH's managed services do not use a client key. They run on FTH's own paid subscriptions or paid API accounts with the providers named above.
- Aggregated insights and statistics that identify no individual are not personal data and are not restricted by this section.
- Before content reaches a model provider, the reviewer's display name and account identifier are replaced by one-way pseudonyms; the profile photo, other media and the anonymity flag are removed; Google's review identifier is replaced by a one-way value; and email addresses and phone numbers are masked. Apart from these steps, the content is sent as it is.
- Masking covers standard formats only: international and local phone numbers, and well-formed email addresses. Other forms, such as digits spelled out in words, Arabic-script numerals, and spaced or

disguised forms, may not be detected. Any item that passes undetected is handled under section 10.

- A name or other detail that a reviewer typed into the public text of a review is not detected by the masking and may reach the provider as part of that text.
- Where a reply addresses the reviewer by name, the FTH staff member preparing the reply adds the name by hand. No software step inserts it, and nothing is sent back to the provider.

5. Hosting and transfers

The platform and its database run on infrastructure provided by Contabo GmbH, established in Germany, within the European Union. The encrypted backups are held in the same provider's object storage within the European Union. FTH Business Manager, Odoo and FTH's dedicated Google Business Profile server run on the same infrastructure, within the European Union. FTH's agreements with Contabo GmbH are data processing agreements under Article 28 of the GDPR, concluded on 24, 29 and 30 August 2026 and covering all FTH's subscriptions with it: compute, object storage and the mail server. Under them, client data is not transferred outside the European Union without FTH's prior consent, and FTH chose server locations within the European Union for all three subscriptions.

Traffic to the platform and to these systems passes through a global edge network operated by Cloudflare, Inc., a company established in the United States. No client data is stored there. Cloudflare's processing is governed by its Customer Data Processing Addendum (version 6.4, 3 April 2026), and its own sub-processors are listed at https://www.cloudflare.com/gdpr/subprocessors/.

Technical operation, development and customer support are performed by FTH personnel, working remotely, including from outside the Kingdom. AI-assisted analysis for FTH's profile recovery, restructuring and management services is performed through model providers in the United States, and for Google also in other countries where Google processes data, on content to which the protection in section 4 has been applied. The providers are listed in section 6.

Processing of personal data outside the Kingdom is subject to the PDPL and the SDAIA Regulation on Personal Data Transfer Outside the Kingdom. **FTH maintains a documented assessment of these transfers, available to the client on request under confidentiality.** FTH gives the client the information it needs for its own transfer assessment. The client, as controller, remains responsible for that assessment.

Risk to data subjects is reduced by the technical measures in section 3.

Deployment inside the Kingdom is available on request, subject to FTH's written approval and to separate commercial terms at the client's cost. FTH may accept or decline a request.

A client that connects its own Google account places that data flow under its own direct and revocable authorisation.

6. Sub-processors

The authoritative list of FTH's sub-processors is the register published at https://fth.marketing/en/subprocessors/ (Arabic: https://fth.marketing/subprocessors/; machine-readable copy: https://fth.marketing/subprocessors.json), reproduced below.

Sub-processor	Purpose	Location
Contabo GmbH	Hosting: servers, database, encrypted backups and email	European Union

Sub-processor	Purpose	Location
Cloudflare, Inc.	Edge network: DNS, protection against attacks, and encrypted connections. Traffic passes through; no data is stored there	Global edge network
MyFatoorah	Subscription payments. Card details are entered on MyFatoorah's own payment page; no card data reaches FTH	Kingdom of Saudi Arabia
Have I Been Pwned	Checks whether a new password appears in known data breaches. Only the first five characters of the password's hash are sent; no personal data is sent	Australia
Anthropic PBC	AI-assisted analysis	United States
Google LLC (Gemini)	AI-assisted analysis	United States and other countries where Google processes data
OpenAI OpCo, LLC	AI-assisted analysis	United States

For the AI providers above: reviewer names and identifiers are replaced by pseudonyms, and photos, email addresses and phone numbers are removed or masked, before content reaches these providers. Details a reviewer writes inside the review text itself may remain. Use of content for model training is turned off, and only paid plans or API accounts are used.

Not sub-processors:

- Services a client contracts directly, such as its own AI key or its own CRM.
- Google, as the source of Business Profile data, accessed with the client's authorisation or as the client's appointed manager of its profiles. Google LLC appears above for Gemini only.
- Software FTH uses to build its products, which does not process client data in the running service.

New or replacement sub-processors are published on the register, and its date changes. A client may object on reasonable data protection grounds within thirty days of a change, as set out in its agreement with FTH. A sub-processor's own sub-contractors are governed by that sub-processor's terms.

7. Retention

Data	Retention
Synced reviews and profile metrics	Kept while the services agreement is active. A review deleted on Google is removed at the next scheduled sync. Erased earlier on request under section 8.
Stored Google access credentials	Deleted immediately when the connected account is disconnected or its authorisation is revoked.
Audit logs	12 months on a rolling basis, then deleted.
Authentication events	90 days on a rolling basis, then deleted. FTH may shorten this period; it cannot be extended beyond 90 days.
Consent records	Kept for as long as the workspace exists, and deleted with it. A record is kept for each decision in both directions, so a withdrawal is itself recorded.

Data	Retention
Review removal requests	A removal request holds a copy of the review it asks Google to take down, so that the outcome can be shown after the review has gone. The request and its copy are deleted 12 months after the request was made, in any state, on the same schedule as audit logs, or earlier with the client's other data when the workspace is deleted at the end of the agreement. The audit trail keeps the record of the request: who asked, who decided, and when.
Diagnostic captures	30 days from capture, deleted by the nightly retention job; deleted immediately when capture is turned off for the workspace.
Reports and exports	Generated on demand and delivered to the requesting user; not kept on the platform.
User account data	Deleted within 90 days of the end of the services agreement. Copies in backups expire on the backup rotation, within about 90 further days. Expired invitations and closed sessions are removed in normal operation.
FTH Business Manager live data (location data, service cases, documents and client-personnel contact details)	Deleted within 90 days of the end of the services agreement, on the same basis as user account data. Its audit and download records identify the FTH staff member who acted, the action and the document type; they hold no document content and no reviewer data, are kept as an audit record for 12 months and then deleted, and are not part of the end-of-agreement deletion.
Call log of FTH's dedicated Google Business Profile server	Each call is recorded with the FTH staff member who made it; kept 12 months, then deleted.
FTH Maps platform database backups	From the start of client services, the local copy is encrypted on the platform host and kept there for 14 days. The off-site copy is encrypted before it leaves the host, held in Contabo object storage within the European Union, and kept as 7 daily, 4 weekly and 3 monthly snapshots, so the oldest is no more than about 90 days old. If no off-site copy can be made on a given night, local copies are not destroyed until an off-site copy succeeds. Erasure under section 8 applies to the live platform immediately; a backup containing an erased record is destroyed on this schedule and is not edited.
FTH Business Manager backups	Every night the database and the files directory are backed up and encrypted (AES-256) before being written to disk; the newest 14 are kept on the host. An encrypted off-site copy is held in Contabo object storage within the European Union as 7 daily, 4 weekly and 1 monthly snapshots. The local copy is restore-tested every night and the off-site copy every week, each recording its result. Backups are not edited; each expires on its fixed rotation, no more than about 35 days after it was made.
Invoices, invoice lines and payment records	Kept indefinitely, with their tax fields, as statutory tax records; not part of the nightly retention job. The billing account's payer address is cleared once no invoice against it is unpaid, and kept while one is.
Error reports (crash and error data)	Not active. The platform sends error events only to an external error-tracking service once one is configured, and any such service is listed as a sub-processor before use. No event leaves the platform. A retention period will be stated here when such a service is configured.

Where the services agreement provides an export window before deletion, that window is added to the periods in this table.

8. Data subject rights and erasure

- Requests from individuals (access, correction, destruction) go to the controller, which holds the relationship with the data subject. FTH, as processor, supports fulfilment within 10 business days of the controller's instruction.
- A reviewer erasure request is carried out by erasing the review record and the analysis records derived from it from the platform, and the erasure is confirmed by an entry in the audit trail. The erasure holds: a later sync of the same branch does not restore the erased review. Erasure also removes any removal-request copy and the classification described in section 2, and clears the erased review's content from the audit entries that recorded it. Where a backup copy is destroyed outside the rolling schedule, its contents are documented before destruction.

9. Responsibility boundary

FTH's responsibility covers its systems and its listed sub-processors. FTH remains responsible to the client for a listed sub-processor's performance of the obligations in this document to the same extent, and within the same limits, as for its own acts under the services agreement. Data the client extracts by any means (file export, API, or integrations with its own systems) is the client's copy, under its responsibility as controller. Where FTH sends data to endpoints the client configures, FTH is responsible for secure delivery to that endpoint.

10. Incidents

On any actual or suspected incident affecting data, FTH notifies the client without undue delay and supports notification to the competent authority within 72 hours under the Implementing Regulations.

11. Version history

Version	Date	What changed
3.2	27 September 2026	Adds FTH Business Manager and FTH's internal systems; adds MyFatoorah, Google (Gemini) and OpenAI to the sub-processors; describes the protection applied before content reaches AI providers, encrypted local and off-site backups, restore tests, logging and retention.
3.1	21 September 2026	Adds reviewer-name storage as a client option, the optional classification and its workspace switch, authentication logging, diagnostic data rules, masking limits, backup periods and the payment provider.
3.0	30 August 2026	Covers FTH's Business Profile services and the FTH Maps platform as an independent product; sets the publication and notice model; describes AI processing for each service, FTH personnel access, diagnostic data and FTH's responsibility for its sub-processors.
2.4	30 July 2026	Earlier issued version.

Privacy enquiries, data subject requests and audit requests: privacy@fth.sa for FTH's Business Profile services, privacy@fth.marketing for its products. Every statement above about FTH's systems can be demonstrated against those systems at publication, and every statement of an FTH rule against FTH's records.