



FTH Data Protection Specifications

Version 3.0, 2026-08-30. Supersedes v2.4 (2026-07-30).

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, accompanied by a change log stating the date and scope of each amendment.

0.3 This document is updated by publication. FTH publishes any addition of a new sub-processor on the sub-processor register page at <https://fth.marketing/en/subprocessors/> (Arabic: <https://fth.marketing/subprocessors/>) and publication constitutes sufficient notice. Section 6 states when FTH may engage it and how a client objection is handled. Clarifications that reduce no existing commitment take effect upon publication.

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

0.5 Contracts reference this document and do not amend it. Any additional commitment agreed with a client is recorded in that client's own contractual documents without diminishing 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 in the capacity of a processor under the Personal Data Protection Law and its regulations, acting on the documented instructions of the client as controller, unless stated otherwise in the description of a specific service.

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

Services, delivered by FTH's Business Profile department alongside the agency's other departments 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 a component 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 to it. Each stands on its own: subscription to one implies subscription to none of the others, 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 within them. FTH's public websites are outside the scope of this document; their handling of visitor data is described in their own privacy notices.

1.6 Reviews and profile performance data are retrieved exclusively through Google's official APIs. The client grants access either by connecting its own Google account directly to the platform, or by granting FTH's managed accounts access to its profiles. Each constitutes 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 maintain the audit trail.

1.9 Beyond the above, FTH collects no payment card data, no government identity documents, and no end-customer lists within these services.

2. Individuals' data

- The reviewer's publicly posted name is stored with the review. It is not shown on any platform screen and is not included in any export. It appears only in the new-review alert notifications sent to the client's own authorised users, and it is erased with the review.
- Filtering and sorting operate 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.
- One optional classification may be recorded against an individual review: an approximate gender, set by hand by an authorised user of the client and never inferred by the platform. No dictionary, no model, no default. It is held apart from the review, is deleted with it, is never shown beside a reviewer's name, and

is reported only as an aggregate in which any group of fewer than five is suppressed. Nothing is recorded unless the client's staff choose to record it.

- 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 the platform

- Per-client isolation is enforced by the database engine itself (forced Row-Level Security), proven by automated tests.
- Stored access credentials encrypted (AES-256-GCM); passwords hashed with argon2id; TLS with strict certificate verification on all platform endpoints.
- Audit trail: every privileged action is recorded in the same transaction, every export or API retrieval is documented (who, when, what), and every displayed figure traces to the API call that produced it. Authentication events (sign-in and failed sign-in) are not yet logged.
- Permissions are per-capability per-user; membership is re-validated on every request.
- Two-factor authentication is available to all accounts, enforceable per workspace at three levels, and required by default on FTH's operator console.
- Support and operations access to a client workspace runs through named platform accounts under per-capability permissions, and opening a client workspace with platform authority records an audit entry in the same transaction as the read. Read-only platform helpers that do not write an audit entry are limited to a closed list enforced by automated tests.
- FTH staff accounts cannot approve changes on the client's behalf; client accounts cannot write to Google. The two authorities are separate by design.
- Nothing is written to the client's Google profiles without the client's approval. Every outbound change passes an approval pipeline, and the approving user and time are recorded.
- Backups of the database are encrypted before they leave the platform host, and the retention periods in section 7 are enforced by an automated job that runs nightly.

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, through its own subscriptions with model providers, in analysing and managing Business Profiles. Where it does so in the course of these services, the provider is reached through FTH's dedicated Google Business Profile server. **Review content reaches the provider de-identified.** Reviewer names and reviewer profile identifiers do not leave the platform on that path, by construction rather than by procedure. FTH does not rely on that provider holding a data processing agreement covering client personal data, because no client personal data is placed in that channel. The provider is 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 today, and AI is off by default. Any AI feature added later, including one that lets a client connect its own model provider key or purchase model usage through FTH, stays off until an

authorised user of the client switches it on for that workspace through an explicit consent step. This document is updated and the update published under section 0 before any such feature can be switched on.

FTH personnel access during the managed services. Delivering profile recovery, restructuring and management requires 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, is recorded in the audit trail, and is subject to the same de-identification control wherever content is sent to a model provider.

Diagnostic data. FTH develops and improves the platform continuously. Where an authorised user of the client enables diagnostic mode, or FTH enables it to investigate a reported fault, the platform records technical detail about the fault which may include client data present at the moment it occurred. That data is used to diagnose and fix the fault and for no other purpose, is retained under section 7, and the rules at the end of this section apply to it as they apply 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 that apply wherever content leaves the platform.

- Consumer AI subscriptions are never used as a channel for client personal data.
- Aggregated insights and statistics that identify no individual are not personal data and are not restricted by this section.
- Masking before any external call covers standard formats only: international and local phone numbers, and well-formed email addresses. Non-standard renderings, including spelled-out digits, Arabic-script numerals, and spaced or otherwise obfuscated forms, may not be detected. Any item that passes undetected remains governed by section 10.
- The reviewer's name is inserted into generated replies locally and never leaves FTH's systems.

5. Hosting and transfers

The platform and its database run on infrastructure operated by Contabo GmbH within the European Union. The encrypted backups are held on the same provider's object storage within the European Union. Traffic to the platform passes through the edge network of Cloudflare, Inc. in the United States. Technical operation, development and customer support are performed by FTH personnel, working remotely including from outside the Kingdom. AI-assisted analysis supporting FTH's profile recovery, restructuring and management services is performed through a model provider in the United States, on de-identified content, as described in section 4. 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 provides 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 by 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

This is the authoritative list. It is published on FTH's sub-processor register at <https://fth.marketing/en/subprocessors/> (Arabic: <https://fth.marketing/subprocessors/>), with a machine-readable copy at <https://fth.marketing/subprocessors.json>, and changes to it are published there.

FTH may engage a new or replacement 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 terminate the service that relies on it. Termination is limited to that service and does not affect the client's other services with FTH. An objection does not suspend the engagement. The sub-processors listed when this register was first published were already engaged at that date, and publication disclosed them.

Platform

Sub-processor	Established in	Role	Processing location	Instrument
Contabo GmbH	Germany	Infrastructure hosting, including object storage holding encrypted backups and the mail server	Platform, database and encrypted backups within the European Union	Data processing agreements under Article 28 of the GDPR, concluded 2026-08-24, 2026-08-29 and 2026-08-30, covering all FTH subscriptions with the provider: compute, object storage and the mail server. They bind the processor under Article 28 GDPR; transfer of client data outside the European Union requires FTH's prior consent, and FTH selected server locations within the European Union for these subscriptions (panel region: EU for all three subscriptions)
Cloudflare, Inc.	United States	Edge network: DNS, denial-of-service protection, TLS termination. Traffic transits the edge; the platform stores no client data there	Global edge network	Cloudflare Customer Data Processing Addendum v6.4 (2026-04-03), with the provider's published sub-processor list at https://www.cloudflare.com/gdpr/subprocessors/

Profile recovery, restructuring and management

Sub-processor	Established in	Role	Processing location	Instrument
Anthropic PBC	United States	AI-assisted analysis supporting FTH's profile recovery, restructuring and management services, through FTH's own subscription	United States	No data processing agreement is relied on for this channel. Content reaches the provider de-identified, per section 4, so client personal data is not placed in it

This register lists FTH's direct sub-processors. A sub-processor's own sub-contractors are governed by that sub-processor's agreement and published list, and a change there does not change this register.

Providers the client contracts directly are not FTH sub-processors. This includes the client's own AI API key and any receiving endpoint the client configures, such as its own CRM. Google is the source platform, accessed under the client's own documented and revocable authorisation, and is not an FTH sub-processor. Tools FTH uses to build and maintain the platform, which do not process client personal data in the running service, are likewise not sub-processors.

7. Retention

Data	Retention
Synced reviews and profile metrics	Retained while the services agreement is active. A review deleted on Google is removed at the next scheduled sync. Erased earlier on request per section 8.
Stored Google access credentials	Deleted immediately when the connected account is disconnected or its authorisation revoked.
Audit logs	12 months on a rolling basis, then deleted.
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 itself has gone. The request and its copy are deleted 12 months after the request was made, on the same schedule as audit logs, whatever the state of the request. The durable record of the request remains in the audit trail: who asked, who decided, and when.
Reports and exports	Generated on demand and delivered to the requesting user; not retained platform-side.

Data	Retention
User account data	Deleted within 90 days of the end of the services agreement. Expired invitations and closed sessions are removed in the ordinary course of operation.
Encrypted database backups	Retained on a rolling schedule and then destroyed. Erasure under section 8 is applied to the live platform immediately, and a backup containing the erased record is destroyed on that schedule rather than being edited in place.

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

8. Data subject rights and erasure

- Requests from individuals (access, correction, destruction) are directed to the controller as the party holding 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 executed by erasing the review record and its derived analysis records from the platform, with the erasure itself confirmed by an entry in the audit trail. The erasure holds: a review erased on request is not restored by a later synchronisation of the same branch. Erasure also removes any removal-request copy and the classification described in section 2. Where a backup copy is to be destroyed outside the rolling schedule, what it contains is documented before destruction.

9. Responsibility boundary

FTH's responsibility covers its systems and its declared sub-processors. FTH remains responsible to the client for a declared 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 pushes data to client-configured endpoints, FTH is responsible for secure delivery to that endpoint.

10. Incidents

On any actual or suspected incident affecting data: client notification without undue delay, and support for notification to the competent authority within 72 hours per the Implementing Regulations.

11. Version history

Version	Date	What changed
3.0	2026-08-30	Rewrote sections 0 and 1 to cover FTH's Business Profile services and its FTH Maps platform product. Established this document as a standalone published specification with its own versioning and notice model (section 0). Corrected the sub-processor register: the hosting account is recorded on evidence and the hosting location is stated at the level the provider's panel evidences, the European Union, the Article 28 agreements concluded on 2026-08-24, 2026-08-29 and 2026-08-30 are recorded, and the operating sub-processor listed in earlier drafts is removed because FTH performs operation, development and support itself. Rewrote section 4 so each service is described on its own: the only AI channel that exists supports profile recovery, restructuring and management, and the control on it is de-identification rather than a contractual instrument. Stated plainly that the platform itself has no AI feature. Recorded the transfer assessment as maintained. Added the retention period for review removal requests. Stated the erasure commitment as durable across synchronisation. Described FTH's structure: three Business Profile services and the FTH Maps platform as an independent product (section 1). Stated FTH's use of AI tools in the managed services as a standing practice rather than a past act. Replaced the flat statement that the platform has no AI feature with the default-off position and the consent step governing any future feature, including a client's own provider key or model usage purchased through FTH. Disclosed FTH personnel

Version	Date	What changed
		access to client accounts during the managed services, and the diagnostic data recorded when fault investigation is enabled. Stated FTH's responsibility for its declared sub-processors, to the same extent and within the same limits as for its own acts (section 9). Restated the sub-processor notice model: publication is the notice, FTH may engage from the date of listing, and a client objection within thirty days is answered by working with the client, by excluding an optional-feature sub-processor from that workspace, or where it is infrastructure and unresolved, by the client terminating the service that relies on it.
2.4	2026-07-30	Previous 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 clause above is demonstrable against the platform.