



Security & Privacy Disclosure, Final Report

Logos Bible Study (com.logos.androidlogos)

A markedly clean scripture app with one real question: two behavioural analytics SDKs and first-party telemetry run over religious-behaviour data with no consent management platform. Nine messages over 73 days drew only automated ticket acknowledgments, and the report is published 18 days after the embargo.

PUBLIC DISCLOSURE, 17 OCTOBER 2026. EMBARGO REACHED 29 SEPTEMBER 2026, NO SUBSTANTIVE REPLY

Target	Faithlife Corporation, Bellingham, Washington, US (Logos Bible Study)
Package	com.logos.androidlogos v51.0.4 (versionCode 1425104003)
Platform analysed	Android, static analysis of the production APK (Xamarin / .NET with AOT), pulled from a retail device on 2026-06-30
First report (R1)	2026-07-01 (REF LOGOS-2026-R1-001)
Embargo date	2026-09-29
Report published	2026-10-17
Overall severity	HIGH
Findings	7 (0 Critical, 2 High, 3 Medium, 2 Low)
Correspondence	9 messages over 73 days to cs@logos.com, 5 identical automated acknowledgments from customerservice@logos.com, 0 human replies, 0 bounces
Authorities in copy	Austrian Data Protection Authority (DSB) from 2026-07-23, European Data Protection Supervisor (EDPS) from 2026-08-09

security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

1	Executive Summary	4
2	Subject & Operator Context	5
3	Architecture & Data Flow	5
4	Correspondence Summary	6
5	Findings	6
5.1	H-1: Two behavioural analytics SDKs and first-party telemetry on religious-behaviour data, no consent management platform	6
5.2	H-2: US telemetry transfer, EU endpoint compiled in with unknown active zone, no Art. 27 representative	7
5.3	M-1: Amplitude location capture capability and precise location permission in a Bible app	8
5.4	M-2: Hardcoded Google / Firebase API key and project identifiers in cleartext	8
5.5	M-3: Cleartext traffic permitted app-wide, no certificate pinning	9
5.6	L-1: Advertising ID permissions and reader present, Google Analytics collection disabled	9
5.7	L-2: Inert IABTCF consent scaffolding without a writing component	10
6	Impact Analysis	10
7	The Complete Chain	10
8	Data Protection, Article by Article	11
9	Regulatory & Legal Landscape	12
10	Indicators of Compromise & Reproducible Evidence	12
11	Disclosure Timeline & Outcome	13
12	Residual Risk & Recommendations	13

Executive Summary

Logos Bible Study is a scripture study application operated by Faithlife Corporation. By its nature it processes special-category data under Art. 9 GDPR, because the passages a user reads, highlights and plans reveal religious conviction.

This report starts with credit. The build contains no ad networks, no Meta SDK, no Chinese or sanctioned SDKs, no attribution SDKs and no session replay, and it disables the advertising ID for Google Analytics. It is markedly cleaner than the other faith apps in the RFI-IRFOS corpus. Its one real exposure is structural: Amplitude, Firebase Analytics and a first-party event system run on that special-category dataset, Firebase initialises before any consent screen, and no consent management platform exists in the build.

The evidence is static. The event producers are AOT-compiled .NET, so the report proves the plumbing and the missing consent gate and does not prove the content of the events. The priority hypothesis is PARTIAL.

RFI-IRFOS reported seven findings on 1 July 2026 and followed up eight times, on 6, 17, 23 and 31 July, 9, 15 and 31 August and 12 September. The only responses on record are five identical automated acknowledgments from the customer service system, received after the follow-ups of 31 July, 9 August, 15 August, 31 August and 12 September. No person at Faithlife engaged with any finding. The embargo of 29 September 2026 passed and this report was published on 17 October 2026.

ID	Severity	Title
H-1	HIGH	Two behavioural analytics SDKs and first-party telemetry on religious-behaviour data, no consent management platform
H-2	HIGH	US telemetry transfer, EU endpoint compiled in with unknown active zone, no Art. 27 representative
M-1	MEDIUM	Amplitude location capture capability and precise location permission in a Bible app
M-2	MEDIUM	Hardcoded Google / Firebase API key and project identifiers in cleartext
M-3	MEDIUM	Cleartext traffic permitted app-wide, no certificate pinning
L-1	LOW	Advertising ID permissions and reader present, Google Analytics collection disabled
L-2	LOW	Inert IABTCF consent scaffolding without a writing component

Subject & Operator Context

Logos Bible Study is the Android application of Faithlife Corporation of Bellingham, Washington. The legal entity appears in the .NET assemblies Faithlife.* and the namespaces Logos.*. Account and authentication hosts are auth.faithlife.com, auth.logos.com and accountsapi.logos.com. The privacy policy is published at faithlife.com/privacy and logos.com/privacy. The Firebase project is mobile-logos-bible. Faithlife is a non-EU operator. RFI-IRFOS found neither an Art. 27 EU representative nor a data protection officer address in the package.

Architecture & Data Flow

The application is a Xamarin / .NET (Mono) app. Application logic is AOT-compiled into native libraries, so managed strings and the first-party event payloads are not readable statically. Third-party SDKs such as Firebase and Amplitude live in Java and Kotlin DEX and are readable. The flow that matters is: process start, then FirebaseInitProvider initialises Firebase Analytics before any consent screen, then Amplitude and the Logos.UserEvents pipeline send telemetry to US and possibly EU endpoints.

What the build gets right:

- No ad networks: AdMob serving, AppLovin, Unity Ads, ironSource and Vungle were all confirmed absent.
- No Meta SDK: only com.facebook.shimmer, a UI loading library, is present.
- No Chinese or sanctioned SDKs: Tencent, ByteDance and Pangle, Umeng, Baidu, Aliyun and Mintegral were all confirmed absent.
- No attribution or marketing SDKs and no session replay: AppsFlyer, Adjust, Branch, Mixpanel, Segment, Iterable and Braze are absent, and the Amplitude Session Replay plugin is not bundled.
- The advertising ID is deliberately disabled for Google Analytics.
- allowBackup is false, the app is not debuggable, and user CA trust is confined to debug-overrides.
- The vast majority of traffic goes to the operator's own logos.com and faithlife.com infrastructure.
- The EU Amplitude endpoint is compiled in, so EU data residency is available if selected.
- No RECORD_AUDIO, contacts, phone state or SMS permissions. The camera is used for ML Kit barcode and text recognition.

Correspondence Summary

RFI-IRFOS sent the first report on 1 July 2026 to cs@logos.com, the only contact address found, and put three questions on the Art. 9(2) exception, on consent before processing, and on the active Amplitude zone and transfer mechanism. Eight follow-ups restated the findings and the questions. The Austrian DSB was copied from 23 July and the EDPS from 9 August. The customer service system answered five of the nine messages with the identical templated acknowledgment, from customerservice@logos.com. The follow-up of 12 September described that pattern accurately: a ticket receipt is an automated receipt and not a response to the findings. No human reply and no bounce occurred at any point.

Findings

H-1: Two behavioural analytics SDKs and first-party telemetry on religious-behaviour data, no consent management platform

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.0

```
AndroidManifest.xml: com.google.firebase.provider.FirebaseInitProvider (auto-init
    ContentProvider)
DEX: Lcom/amplitude/core/*, Lcom/amplitude/android/*
DEX: Lcom/google/android/gms/measurement/AppMeasurement, AppMeasurementContentProvider
no firebase_analytics_collection_deactivated flag present
.NET: Logos.UserEvents.Client / .Manager / .Contracts (arm64 split)
CMP classes (OneTrust, Usercentrics, Didomi, UMP, TCF): 0
```

Why this matters for this product. In a scripture study app, the passages a person reads, their highlights, notes, reading plans and study activity reveal religious conviction, which is special-category data under Art. 9(1) GDPR. Processing it needs an Art. 9(2) exception, and explicit consent under Art. 9(2)(a) is hard to evidence when the build has no consent platform.

Limits of this finding. The event producers are AOT-compiled .NET and cannot be read statically. RFI-IRFOS therefore proved the plumbing and the missing consent gate and did not prove that specific scripture, highlight or prayer events are placed in the Amplitude or Firebase payloads. That question was reserved for dynamic analysis and put to the operator as question 2. The priority hypothesis stands at PARTIAL.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.0 to HIGH because the affected dataset is special-category religious behaviour, the collection starts before any consent screen, and the app serves a global user base.

Impact: The build bundles the Amplitude product analytics SDK and Firebase Analytics, and a first-party event system (Logos.UserEvents.Client, Manager and Contracts). Firebase Analytics runs with no deactivation flag, so collection is on by default. FirebaseInitProvider is a ContentProvider that initialises at process start, before any consent screen. No consent management platform is present: OneTrust, Usercentrics, Didomi, Google UMP and

TCF classes are all absent, and the IABTCF preference keys exist only as inert SDK constants that nothing writes.

H-2: US telemetry transfer, EU endpoint compiled in with unknown active zone, no Art. 27 representative

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.0

```
https://api2.amplitude.com/2/httpapi, /batch
diagnostics.prod.us-west-2.amplitude.com
https://api.eu.amplitude.com/... (also compiled in)
diagnostics.prod.eu-central-1.amplitude.com
firebase-settings.crashlytics.com
com.google.android.datatransport.cct.CctBackendFactory
Lcom/amplitude/core/ServerZone (runtime region selection)
```

Limits of this finding. Which ServerZone is active in production cannot be determined statically. Shipping the EU endpoint is a real mitigation if it is selected. If the US zone is active, transferring religious-behaviour telemetry engages Art. 44 ff. GDPR and needs a transfer mechanism such as Standard Contractual Clauses or Data Privacy Framework coverage, plus disclosure under Art. 13(1)(f). Question 3 to the operator asked exactly this.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.0 to HIGH because religious-behaviour telemetry is the most sensitive category of data the app can generate and a US routing path exists for it.

Impact: The binary contains the US Amplitude endpoint `api2.amplitude.com` and also the EU endpoint `api.eu.amplitude.com`. The class `com.amplitude.core.ServerZone` selects the region at runtime. Firebase Crashlytics settings and the `datatransport CCT` backend route to Google infrastructure in the United States. The operator, Faithlife Corporation, is a US entity. RFI-IRFOS found no EU representative in the package or in the privacy policy.

M-1: Amplitude location capture capability and precise location permission in a Bible app

LOW, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3

Limits of this finding. The capability is confirmed. Whether locationListening is enabled at runtime, and which legitimate feature such as a Biblical atlas or church finder justifies precise location, was not determined and is a question for the operator. If it is enabled, each religious-behaviour event could carry precise coordinates.

RFI-IRFOS blast-radius escalation: raised from LOW/2.3 to MEDIUM because precise location combined with religious-behaviour events would create a particularly sensitive profile.

Impact: The manifest declares ACCESS_FINE_LOCATION and ACCESS_COARSE_LOCATION. The Amplitude SDK in the DEX exposes locationListening, trackingOptions, Latitude and Longitude, which is the option that attaches device coordinates to analytics events. The app also references android.location.Geocoder and LocationManager.

M-2: Hardcoded Google / Firebase API key and project identifiers in cleartext

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9

```
google_api_key      = [REDACTED IN PUBLIC REPORT, disclosed privately to Faithlife Corporation in R1]
google_app_id       = [REDACTED IN PUBLIC REPORT, disclosed privately to Faithlife Corporation in R1]
project_id          = [REDACTED IN PUBLIC REPORT, disclosed privately to Faithlife Corporation in R1]
firebase_database_url = [REDACTED IN PUBLIC REPORT, disclosed privately to Faithlife Corporation in R1]
google_storage_bucket = [REDACTED IN PUBLIC REPORT, disclosed privately to Faithlife Corporation in R1]
```

Limits of this finding. A Firebase key is designed to be embedded, and RFI-IRFOS did not send any request with it. The open question is whether the key carries API restrictions and whether the Firestore, Realtime Database and Storage rules are locked. If they are not, the key can enable quota abuse and unwanted backend access. The operator carries the burden of showing the key is scoped and the rules are closed.

Impact: res/values/strings.xml in the production APK contains a Google API key, the Google app identifier, the project identifier, the Firebase database URL and the storage bucket in cleartext. Any user who downloads the app can extract them.

M-3: Cleartext traffic permitted app-wide, no certificate pinning**MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3**

```
<base-config cleartextTrafficPermitted="true">
  <trust-anchors>
    <certificates src="@raw/isrg_root_x2" />
    <certificates src="@raw/isrg_root_x1" />
    <certificates src="system" />
  </trust-anchors>
</base-config>
```

Recommendation: set cleartextTrafficPermitted to false and pin the telemetry and API hosts.

Impact: The network security configuration sets cleartextTrafficPermitted to true in its base-config, which allows plaintext HTTP for any domain without a more specific rule. No pin-set is configured. The app trusts the ISRG roots and the system store, which is trust anchoring and not pinning. User CA trust is confined to debug-overrides, which is correct.

L-1: Advertising ID permissions and reader present, Google Analytics collection disabled**LOW, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3**

Limits of this finding. Whether Amplitude reads the advertising ID as a device identifier was not determined. The deliberate Google Analytics opt-out is a genuine privacy-positive signal.

Impact: The manifest declares ACCESS_AD SERVICES_AD_ID and ACCESS_AD SERVICES_A TTRIBUTION, and the AdvertisingIdClient class is present. google_analytics_adid_collection_enabled is set to false, so Firebase Analytics is told not to collect the advertising ID. No ad serving classes exist.

L-2: Inert IABTCF consent scaffolding without a writing component

LOW, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3

Limits of this finding. Consent may be handled in the .NET user interface, which is not readable statically. The observation reinforces H-1 and is informational.

Impact: IABTCF keys (IABTCF_CmpSdkID, IABTCF_TCString, IABTCF_gdprApplies, IABTCF_PurposeConsents, IABTCF_EnableAdvertiserConsentMode) exist as SDK constants. No consent SDK is present that could populate them. The SDKs can read a consent string, but nothing in the build collects one at the SDK layer.

Impact Analysis

Every user of the app is affected. Their reading activity is the product's core data and it reveals religious belief. Collection by the analytics SDKs begins at process start without a consent decision. If the US Amplitude zone is active, that telemetry reaches US infrastructure. For a user the practical consequence is that a record of how they study scripture may exist at third-party analytics providers without a lawful basis they were asked to confirm. The operator has not said which basis it relies on.

The Complete Chain

A user installs Logos Bible Study and opens it. At process start, FirebaseInitProvider initialises Firebase Analytics, which is enabled by default. Amplitude and the first-party Logos.UserEvents pipeline are present in the same process. No consent management platform exists in the build, so no consent decision can gate any of them at the SDK layer. As the user reads passages, highlights text and follows reading plans, the product generates the data that reveals religious conviction. The Amplitude client can send events to api2.amplitude.com in the United States or to api.eu.amplitude.com, depending on a runtime zone that the binary does not reveal. The content of those events is the one link in this chain that static analysis cannot prove, and RFI-IRFOS says so. When the researcher reports the structure and asks three questions, the operator's system returns an automated receipt five times and nothing else.

Data Protection, Article by Article

Article	Engaged by	Finding
Art. 5(1)(a)	Lawfulness and transparency of analytics on religious data	H-1
Art. 5(1)(c)	Minimisation, location capability and advertising ID reader	M-1, L-1
Art. 6(1)	Lawful basis for analytics at process start	H-1
Art. 7(1)	Proof of consent, no consent platform, inert IABTCF scaffolding	H-1, L-2
Art. 9(1)-(2)	Religious behaviour as special-category data, exception not stated	H-1, M-1
Art. 13(1)(f)	Disclosure of third-country transfer	H-2
Art. 27	No EU representative found	H-2
Art. 32(1)	Hardcoded key and cleartext traffic permitted	M-2, M-3
Art. 44-49	US telemetry endpoint, transfer mechanism not stated	H-2

Regulatory & Legal Landscape

Faithlife has no EU establishment that RFI-IRFOS could identify, so the one-stop-shop mechanism does not apply cleanly. RFI-IRFOS proposed the Austrian Data Protection Authority as the lead point of contact for the report because RFI-IRFOS is established in Austria, and copied the DSB and the EDPS. Any EU data subject can complain to the authority of their residence. Compared with the other faith apps in the RFI-IRFOS corpus, which carried ad networks, the Meta SDK and Chinese SDKs, Logos is substantially cleaner. Compared with benchmark apps that ship no analytics at all, it is dirtier, because it runs dual product analytics without a visible consent gate.

Indicators of Compromise & Reproducible Evidence

```
package:          com.logos.androidlogos
version:          51.0.4 (versionCode 1425104003, minSdk 32, targetSdk 36)
base APK sha256:  733540d4c46bec5f2a9c33343cc2ac5943ace9f26ac89e1eb1ab9df5545e4892
                  (80,786,762 bytes)
arm64 split sha256: 4baa9350f5d9663c5ee093611a4cd3ce8c092b0b7d5eaf054c2e35fdb0bf3639
                  (43,037,925 bytes)
source:           retail device, 2026-06-30
method:           apktool (manifest, resources, network security config), strings and
                  grep over classes*.dex, AOT .so inspection
endpoints:        api2.amplitude.com, api.eu.amplitude.com, firebase-settings.
                  crashlytics.com
keys:             redacted in this public report, disclosed privately in R1
```

A second researcher can reproduce every item by unpacking the stated APK and checking the manifest provider, the DEX namespaces and the network security configuration.

Disclosure Timeline & Outcome

2026-06-30 Version 51.0.4 pulled from a retail device and analysed statically.

2026-07-01 R1 sent to cs@logos.com. Seven findings, three questions. Embargo 2026-09-29. REF LOGOS-2026-R1-001.

2026-07-06, 2026-07-17 First and second follow-up. No reply.

2026-07-23 Third follow-up, Austrian DSB in copy. No reply.

2026-07-31 Fourth follow-up, DSB in copy. Automated acknowledgment received.

2026-08-09 Fifth follow-up, DSB and EDPS in copy. Automated acknowledgment received.

2026-08-15 Sixth follow-up, DSB and EDPS in copy. Automated acknowledgment received.

2026-08-31 Seventh follow-up, DSB and EDPS in copy. Automated acknowledgment received.

2026-09-12 Eighth follow-up, answer deadline 2026-09-24. Automated acknowledgment received.

2026-09-29 Embargo date reached, as stated in R1 and never revised. Correspondence status: nine RFI-IRFOS messages, five identical automated acknowledgments, no human reply, no bounce.

2026-10-17 This report published, 18 days after the embargo date.

Residual Risk & Recommendations

All seven findings are open as of publication. RFI-IRFOS recommends that Faithlife introduce a consent management platform that gates Firebase, Amplitude and the Logos.UserEvents pipeline before process start, state the Art. 9(2) exception it relies on, confirm the active Amplitude ServerZone and the transfer mechanism, designate an Art. 27 representative, restrict the Google API key and review the Firebase rules, set cleartextTrafficPermitted to false and pin the API hosts. Dynamic analysis of the event payloads remains open and would settle the one unproven link in the chain. RFI-IRFOS will record any substantive reply from Faithlife next to the original findings in the public dataset, whenever it arrives.

RFI-IRFOS security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria All findings rest on static analysis of the published

application with publicly available tools. No Faithlife, Amplitude or Google servers, accounts or infrastructure were tested. Technical evidence is archived under chain of custody and is available to supervisory authorities on request. Research conducted under ISO/IEC 29147, the freedom of science (Art. 17 StGG) and GDPR Art. 89. REF LOGOS-2026-R1-001.