Data-Flow Privacy Audit - ExampleFit (fictional)

EXAMPLE, fictional data. The app, company, findings and evidence are invented for demonstration only.

Field | Value

Client | ExampleFit Ltd. (fictional)

App | ExampleFit 4.2.0 (iOS), 4.2.1 (Android)

Test period | 3-14 Nov 2026 (fictional)

Auditor | SILENCE.OBJECTS

Report version | 1.0

1. Executive summary

During testing the app sent data to 9 external domains belonging to 6 vendors. We identified 3 high-risk findings:

1. Meta SDK sends events with a device identifier BEFORE the user gives consent in the banner (iOS and Android).
2. Weight and fitness goal (potential health data) are sent to Firebase Analytics as event parameters; the privacy policy does not describe this.
3. The App Store label declares "Data Not Linked to You" for health data, while traffic shows it linked to the user ID.

All three can be fixed with SDK configuration and text changes, an estimated 3-5 team days (ASSUMPTION).

2. Scope and method

In scope: iOS and Android builds from TestFlight / APK, test accounts, privacy policy (version of 1 Oct 2026), App Store "App Privacy" label, Google Play "Data safety".

Out of scope: client servers, penetration testing, real user data, certification.

Method: (1) static analysis (MobSF, apktool, Exodus Privacy signatures); (2) traffic capture (mitmproxy; test iPhone via proxy, Android emulator) on 11 paths: install, consent banner (accept / decline), sign-up, login, profile, workout, payment, sharing, logout, account deletion; (3) comparison with policy and labels; (4) risk ranking.

Limitations: api.examplefit.example uses certificate pinning; only domain names are visible, not content. Traffic outside the tested paths may not be captured.

3. Data-flow table

 # | Destination | SDK / vendor | Data fields | Purpose | In policy? | Label match | Risk | Evidence

F1 | graph.facebook.com | Meta SDK | IDFA/AAID, app_open event, device model | ads / attribution | Y | N (before consent) | H | E-01, E-02

F2 | app-measurement.com | Firebase Analytics | app_instance_id, weight_kg, goal | analytics | N | N | H | E-03

F3 | firebaseinstallations.googleapis.com | Firebase Installations | FID, app version | technical | Y | Y | L | E-04

F4 | api.revenuecat.com | RevenueCat (payments) | app_user_id, product, price | subscriptions | Y | Y | L | E-05

F5 | o12345.ingest.sentry.io | Sentry | stack trace, email in breadcrumbs | crash reports | Y (general) | N | M | E-06

F6 | api.mixpanel.com | Mixpanel | distinct_id = user_id, screen, workout time | product analytics | Y | N (linked to user) | H | E-07

F7 | maps.googleapis.com | Google Maps SDK | approximate location | route map | Y | Y | M | E-08

F8 | cdn.examplefit.example | own CDN | no personal data | content | n/a | n/a | L | E-09

F9 | api.examplefit.example | client backend | [pinning - content not visible] | core app | Y | ? | M | E-10

EXAMPLE, fictional data

4. Findings

U-1 (H): Meta SDK before consent

On first launch, before the banner is shown, the event fb_mobile_activate_app is sent with the advertising identifier. Evidence E-01: [SCREENSHOT: mitmproxy, POST graph.facebook.com/.../activities, 00:00:02 after launch]. Evidence E-02: [SCREENSHOT: consent banner shown at 00:00:04].

U-2 (H): Weight and goal data in Firebase

Parameters weight_kg and goal=lose_weight in the profile_saved event. These may be data concerning health (GDPR Art. 9). Evidence E-03: [REQUEST EXCERPT: params: {weight_kg: 7*, goal: "lose_..."} - masked].

U-3 (H): Mismatch with App Store label

Label: "Health & Fitness - Data Not Linked to You". Mixpanel receives distinct_id equal to the account ID together with workout time. Evidence E-07: [SCREENSHOT of App Store label + request to api.mixpanel.com/track].

U-4 (M): Email in Sentry crash reports

Breadcrumbs contain the email address from the login form. Evidence E-06: [EXCERPT: breadcrumb "login_form: an***@example.com"].

U-5 (M): Declining consent does not stop Mixpanel

After tapping "Decline", Mixpanel events are still sent (Android). Evidence E-07b: [SCREENSHOT: 14 requests after decline].

U-6 (L): RevenueCat not named in the policy

The policy mentions a "payment provider" without its name or country of processing.

5. GDPR risk ranking

NOT LEGAL ADVICE. Technical assessment pointing to areas for review by the client's counsel.

 # | Finding | GDPR / regulatory area | Risk

1 | U-2 | possible special-category data (Art. 9), legal basis, transparency (Art. 13) | High

2 | U-1 | consent before device access (ePrivacy / GDPR Art. 6), transfer outside EEA | High

3 | U-3 | consistency with App Store declaration (Apple guidelines 5.1.1/5.1.2) | High

4 | U-5 | effective withdrawal of consent (Art. 7(3)) | Medium

5 | U-4 | data minimisation (Art. 5(1)(c)) | Medium

6 | U-6 | transparency of recipients (Art. 13(1)(e)) | Low

6. Fix list (priorities)

Prio | Fix | Owner | Effort (ASSUMPTION)

P1 | Delay Meta SDK init until consent (AutoInitEnabled=false, AdvertiserIDCollectionEnabled=false) | iOS/Android | 0.5 day

P1 | Remove weight_kg/goal from Firebase parameters or move to backend | mobile | 0.5 day

P1 | Correct App Store label and Data safety ("Linked to You") or anonymise Mixpanel | product | 0.5 day

P2 | Stop Mixpanel after decline (optOutTracking()) | Android | 0.5 day

P2 | Sentry beforeBreadcrumb filter removing email | mobile | 0.5 day

P3 | Name recipients and countries in the privacy policy | legal | 1 day

P3 | Provide a test build without pinning to re-test F9 | backend | 0.5 day

7. Annexes

A. SDK list (static): Meta SDK 17.x, Firebase Analytics 11.x, Firebase Crashlytics (detected, inactive in traffic), RevenueCat 5.x, Sentry 8.x, Mixpanel 4.x, Google Maps 9.x - fictional versions.

B. Android permissions: INTERNET, ACCESS_COARSE_LOCATION, AD_ID, POST_NOTIFICATIONS.

EXAMPLE, fictional data

C. Environment: test iPhone iOS 18.x; Android 14 emulator (no Google Play image, rooted); mitmproxy 11.x; MobSF 4.x.

D. Evidence register E-01...E-10: delivered as a separate, masked package.

E. Disclaimer: technical review, not a certification, not a penetration test, not legal advice. Test data deleted 30 days after delivery.

EXAMPLE, fictional data

EXAMPLE, fictional data