Security & Privacy Disclosure, Final Report

Medikhata: Health Report AI (in.medikhata.app)

A family health-records app whose own text denies sharing health data, admits an unnamed AI processor, and starts Firebase and Facebook before any consent.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED

Target	Medikhata: Health Report AI. Google Play developer: Aivorn Technology and Consulting. Legal text names the brand Medikhata, Mumbai, India.
Notice / Publication	2026-08-21 / 2026-11-19 (90 days, unchanged)
Versions Audited	1.0.5 / versionCode 25 (analysed 2026-08-21)
Findings	9: 2 Critical, 2 High, 5 Medium
Regulators in copy	Austrian DSB and EDPS (first notice)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026

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

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

Contents

1 Executive Summary 3

2 Finding Status at a Glance 4

3 Subject & Operator Analysis 5

4 Architecture & Data Flow 5

5 Engagement Summary 6

6 Findings 6
- 6.1 C1: App text denies sharing health data and admits an unnamed AI processor 6
- 6.2 C2: Firebase and Facebook SDKs start before any consent, no consent platform 8
- 6.3 H1: AD_ID permission and Facebook event logger against a never-for-advertising claim 9
- 6.4 H2: Firebase API key hardcoded, Storage bucket name exposed 10
- 6.5 M1: No operator identity, personal Gmail as privacy contact, legal address on another domain 11
- 6.6 M2: Play Data Safety lists health info for Analytics, against the FAQ 12
- 6.7 M3: No Article 27 representative while installable in Austria 13
- 6.8 M4: Fine and coarse location permissions with no identified in-app feature 13
- 6.9 M5: One identity across three sign-in routes, no age handling for dependents 14

7 Impact Analysis 15

8 The Complete Chain 15

9 Child Protection & Dependent Profiles 16

10 Data Protection: Article by Article 16

11 Consumer Protection & Platform Disclosures 17

12 Regulatory & Legal Landscape 17

13 Indicators of Compromise & Reproducible Evidence 17

14 Disclosure Timeline & Outcome 18

15 What Medikhata Got Right 19

16 Residual Risk & Recommendations 19

Executive Summary

Medikhata: Health Report AI (in.medikhata.app) is a Flutter app in which families store lab reports, prescriptions and uploaded documents behind phone, Google or Facebook sign-in, with an Ask Medikhata AI chat over that data. The Play listing showed an update dated 18 July 2026. On 21 August 2026 RFI-IRFOS disclosed nine findings from a root level code analysis of version 1.0.5 under REF MEDIKHATA-2026-R1.

The central finding is a contradiction inside the shipped app. The in-app Privacy Policy text says health data is shared with third-party processors for AI-assisted report analysis and authentication infrastructure. Two FAQ answers in the same binary say health data is stored on the device and is never shared without consent. The app sends documents and chat content to its own backend at api.medikhata.in, and no AI vendor endpoint appears in the client, so the processor the policy mentions is not named anywhere that RFI-IRFOS could read.

Two further facts shape the case. Firebase and the Facebook SDK start as ContentProviders before any screen can ask for consent, and no consent platform exists in the build. And the operator is hard to identify: Google Play names Aivorn Technology and Consulting, the app's own legal text names only the brand Medikhata with a city-level address, the privacy contact is a private Gmail mailbox, and no Art. 27 representative is named although the app is installable in Austria.

RFI-IRFOS sent the notice to medikhataai@gmail.com and support@medikhata.in with the Austrian DSB and the EDPS in copy. The support@ address failed permanently on 24 August 2026. A follow-up went out on 5 September 2026 and a reminder on 17 October 2026. No substantive reply has arrived as of 14 November 2026. Publication stays at 19 November 2026, independent of any reply. The analysis is static and no server-side behaviour was examined, so the report states what the binary and the operator's own texts show and marks what it cannot show.

Scope: Root level code analysis of Medikhata: Health Report AI, version 1.0.5 (versionCode 25), base APK and XAPK bundle obtained from the APKCombo mirror because the app was not installed from Google Play: manifest, resources, dex string pool and the Flutter AOT library libapp.so (arm64-v8a). The package carries a generic Google distribution signing certificate, which fits a Play-signed release fetched through a mirror. Version, developer name and the update date were cross-checked against the live Play listing. The signer certificate was not compared with a second copy. Public web pages read by plain HTTP GET on 21 August 2026: the Play listing, the Data Safety page, and the privacy policy, terms and About page at medikhata.in. No backend endpoint was called, no key was used, no account was created, no traffic was intercepted and no runtime instrumentation was used.

ID	Severity	Title
C1	CRITICAL	App text denies sharing health data and admits an unnamed AI processor
C2	CRITICAL	Firebase and Facebook SDKs start before any consent, no consent platform
H1	HIGH	AD_ID permission and Facebook event logger against a never-for-advertising claim
H2	HIGH	Firebase API key hardcoded, Storage bucket name exposed
M1	MEDIUM	No operator identity, personal Gmail as privacy contact, legal address on another domain
M2	MEDIUM	Play Data Safety lists health info for Analytics, against the FAQ
M3	MEDIUM	No Article 27 representative while installable in Austria
M4	MEDIUM	Fine and coarse location permissions with no identified in-app feature
M5	MEDIUM	One identity across three sign-in routes, no age handling for dependents

Finding Status at a Glance

ID	Severity	CVSS-B	Status on 14 November 2026
C1	CRITICAL	0.0	Not answered. Open.
C2	CRITICAL	6.9	Not answered. Open.
H1	HIGH	6.9	Not answered. Open.
H2	HIGH	6.9	Not answered. Open.
M1	MEDIUM	0.0	Not answered. Open.
M2	MEDIUM	0.0	Not answered. Open.
M3	MEDIUM	0.0	Not answered. Open.
M4	MEDIUM	4.6	Not answered. Open.
M5	MEDIUM	0.0	Not answered. Open.

Subject & Operator Analysis

Google Play lists the app under the developer name Aivorn Technology and Consulting. That name does not appear in the application binary, in the Privacy Policy, in the Terms and Conditions or on the About page at medikhata.in. Those pages present the trading brand Medikhata. The structured data on the privacy page declares an Organization named Medikhata with the contact support@medikhata.in and the locality Mumbai, Maharashtra, India. No company suffix, no registration number and no governing-law or jurisdiction clause appears in the Terms.

The Privacy Policy names a Medikhata Privacy Office reachable at a free Gmail address. The binary contains a legal contact, legal@medikhata.com, on a domain that differs from the app's operating domain. No data protection officer and no EU representative is named in any source RFI-IRFOS read. Which legal person is the controller under Art. 4(7) GDPR therefore remains an open question that the operator can answer in one sentence. The notice asked it.

The Austrian Datenschutzbehörde is the authority RFI-IRFOS would approach for an Austrian-initiated matter, because no EU establishment of the controller was identified.

Architecture & Data Flow

The app is written in Flutter. Business logic is compiled to native code in libapp.so (12.3 MB for arm64). The Android layer holds only plugin glue: Firebase, the Facebook SDK, Google Sign-In, Play Billing, geolocator, pdfium and file and image pickers. minSdkVersion is 24 and targetSdkVersion is 36.

Sign-in runs through Firebase Auth with three routes: phone OTP, Google and Facebook. All three resolve to one account that holds the health records. The app talks to a self-hosted backend at api.medikhata.in for registration, token refresh, uploads, chat, health updates and notification settings. The privacy text and the uploads endpoint show that lab reports, prescriptions and images leave the device. Local PDF rendering with pdfium means basic viewing does not need a round trip, but extraction of report content does.

Firebase Messaging, Installations and App Check client libraries are registered, the Facebook SDK is present with its event logger, and a Play Billing subscription named Medikhata Pro is the visible revenue path. The client contains no AI vendor endpoint. Whatever the AI-assisted analysis does after an upload therefore happens on the operator's servers or at a processor behind them. The hosting location of api.medikhata.in was not examined in this review.

Engagement Summary

The first notice went out on 21 August 2026 to medikhataai@gmail.com and support@medikhata.in with the Austrian DSB and the EDPS in copy, and asked for answers to three questions within 14 days. Mail to support@medikhata.in failed permanently on 24 August 2026. No failure was reported for the Gmail address. A follow-up on 5 September 2026 and a reminder on 17 October 2026 went to the Gmail address. No reply of any kind has arrived as of 14 November 2026.

Findings

C1: App text denies sharing health data and admits an unnamed AI processor

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B)

Three strings in the compiled Dart binary (libapp.so) cannot all describe the same system. The in-app Privacy Policy text says health data is shared with third-party processors for AI-assisted report analysis and authentication infrastructure. Two FAQ answers on the Help and Support screen say health data is stored on the device and is never shared without consent. No processor is named in the binary, on the public privacy policy or on the Play listing.

```
Privacy Policy screen (adjacent class PrivacyDataWidget):
"Health data is shared with third-party processors only where necessary to provide the
service (for example, AI-assisted report analysis and authentication infrastructure),
under contractual safeguards, and never for advertising."

FAQ (faq_resources_widget.dart):
"We take your privacy seriously. Your health data is stored securely on your device.
    We
do not sell, share, or distribute your personal health information to third parties
without your explicit consent. Please refer to our Privacy Policy for detailed
    information."

"Yes, we use bank-level encryption and comply with Indian data protection laws. Your
data is never shared without consent."
```

```
https://api.medikhata.in/api/chat
https://api.medikhata.in/api/uploads
https://api.medikhata.in/api/uploads/file/
https://api.medikhata.in/api/uploads/user/
https://api.medikhata.in/api/health/update/
https://api.medikhata.in/api/register
https://api.medikhata.in/api/refresh-token
https://api.medikhata.in/api/logs/log-otp-event
https://api.medikhata.in/api/notifications/toggle
```

The client sends uploaded documents and chat content to the operator's own backend at api.medikhata.in. A targeted search of both classes*.dex files and libapp.so for openai, gpt-, anthropic, generativelanguage, azure, cognitive and bedrock returned no hits, so no AI vendor endpoint is called from the client. The processor named in the privacy text therefore sits behind api.medikhata.in and cannot be identified from the app.

Limits of this finding. RFI-IRFOS did not call api.medikhata.in and did not observe what happens to an upload after it leaves the device. The identity and location of the AI processor, and the legal basis on which it receives health data, were not determined. The finding rests on the contradiction between the operator's own texts and on the endpoints that show documents and chat leaving the device.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to CRITICAL because the app stores family health records, lab values and prescriptions, which are Art. 9 special-category data. The contradiction answers exactly the question a user asks before uploading, whether the document leaves the phone, and the recipient of the documents is not named anywhere. CVSS gives a pure transparency failure of this kind 0.0.

Impact: A person who reads the Help screen before uploading a parent's or a child's lab report is told the data stays on the device and is never shared without consent. The Privacy Policy screen of the same build says health data goes to third-party processors for AI report analysis and names none. The user cannot learn who receives the documents or where.

Fix: Decide which statement is true and remove the other. Name every processor that receives health data (Art. 13(1)(e)), state the transfer mechanism if any recipient sits outside the EEA (Art. 44 and 46), and document the Art. 6(1) basis together with the Art. 9(2) condition that covers the AI analysis.

C2: Firebase and Facebook SDKs start before any consent, no consent platform

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 (CVSS-B)

FirebaseInitProvider (directBootAware, initOrder 100), FlutterFirebaseMessagingInitProvider (initOrder 99) and Facebook's FacebookInitProvider are ContentProviders. Android runs them during Application creation, before any Activity, so before any consent interface the app could show. A search of libapp.so and both dex files for OneTrust, Didomi, Usercentrics, IABTCF, consentmanager, cmpsdk and TCF strings returned zero matches. The manifest sets only com.facebook.sdk.ApplicationId and com.facebook.sdk.ClientToken for the Facebook SDK. It does not override AutoInitEnabled, AdvertiserIDCollectionEnabled or the app-event logging flag, so they run at the SDK defaults.

```
<provider android:authorities="in.medikhata.app.firebaseinitprovider"
          android:directBootAware="true" android:exported="false"
          android:initOrder="100" android:name="com.google.firebase.provider.
    FirebaseInitProvider"/>
<provider android:authorities="in.medikhata.app.flutterfirebasemessaginginitprovider"
          android:exported="false" android:initOrder="99"
          android:name="io.flutter.plugins.firebase.messaging.
    FlutterFirebaseMessagingInitProvider"/>
<provider android:authorities="in.medikhata.app.FacebookInitProvider"
          android:exported="false" android:name="com.facebook.internal.
    FacebookInitProvider"/>
ComponentDiscoveryService (directBootAware) registers FirebaseAuth, FirebaseMessaging,
FirebaseAppCheck, FirebaseInstallations, FirebaseCommon, datatransport
```

Limits of this finding. The analysis is static. RFI-IRFOS did not capture traffic and did not measure which identifiers Firebase or Facebook transmit at launch. The finding establishes that these SDKs start before any consent mechanism and that no mechanism exists in the build to stop them.

The Play Data Safety page (finding M2) lists Device or other IDs as collected for Analytics, which fits the identifiers these SDKs handle.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to CRITICAL because the app is a health-records product, so a consent choice is the precondition for processing Art. 9 data around it, and the build offers no mechanism to obtain or honour one. The same missing mechanism covers every launch of every install.

Impact: On first launch of an app built to hold lab reports and prescriptions, Google and Facebook SDKs are already running and handling device identifiers, and nothing in the build lets a user decline them first.

Fix: Disable automatic initialisation in the manifest for the Facebook SDK (AutoInitEnabled, AutoLogAppEventsEnabled and AdvertiserIDCollectionEnabled set to false) and for Firebase Analytics collection, then start them from code only after a recorded consent choice.

H1: AD_ID permission and Facebook event logger against a never-for-advertising claim

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 (CVSS-B)

The manifest requests com.google.android.gms.permission.AD_ID and the dex files bundle Facebook's AppEventsLogger, AppEventsLoggerImpl and AppEventsLoggerUtility with the persisted-events store. The privacy text says health data is shared "never for advertising". No evidence was found that report content is passed to an advertising SDK, so that sentence may be accurate in its narrow sense. The advertising identifier itself, however, is requested by design, and the live Data Safety page lists Device or other IDs for Analytics.

```
<uses-permission android:name="com.google.android.gms.permission.AD_ID"/>

Lcom/facebook/appevents/AppEventsLogger;
Lcom/facebook/appevents/AppEventsLoggerImpl;
Lcom/facebook/appevents/internal/AppEventsLoggerUtility;
"AppEventsLogger.persistedevents"
```

Limits of this finding. RFI-IRFOS did not observe whether the advertising identifier leaves the device for an EU user. No feature was found that needs it. The app has no ad-mediation stack, and its main revenue path is a Play Billing subscription, which makes the permission harder to explain.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the permission and the logger sit in an app that stores Art. 9 data and whose own text promises that health data is never used for advertising. A reader reasonably takes that promise to cover the identifier as well.

Impact: The advertising identifier of a person who keeps family medical records is available to the Facebook SDK from the first launch, in an app that tells that person health data is never used for advertising.

Fix: Remove the AD_ID permission if no feature needs it. If Facebook App Events is needed, gate it behind consent and keep it away from screens that show health content.

H2: Firebase API key hardcoded, Storage bucket name exposed

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

res/values/strings.xml contains the Firebase API key for project medikhata-auth, the app ID, the sender ID and the storage bucket medikhata-auth.firebasestorage.app. Google documents that Firebase API keys are not secrets by design. The exposure is therefore one of availability and configuration: an extracted key can be used against the project's quotas, and whether the Storage and Auth rules restrict access per user depends on server-side settings that the binary does not show.

```
google_api_key                AIzaSyB3aIcmPGjmqhOifIbAj8mlnNTdlOokfTo
google_crash_reporting_api_key [same value as google_api_key]
google_app_id                 1:190353699967:android:5f5a462acb08dae151fb4a
project_id                    medikhata-auth
google_storage_bucket         medikhata-auth.firebasestorage.app
gcm_defaultSenderId           190353699967
facebook_app_id               1841379369778337
facebook_client_token         fc85a54585a420983480845d5ea0c667
```

What is not established. The client sends uploads to api.medikhata.in/api/uploads (finding C1). It was not determined whether uploaded documents are also stored in the Firebase Storage bucket. RFI-IRFOS sent no request with the key, tested no Storage or Realtime Database rules and made no statement about their configuration. The App Check client libraries are registered in the manifest. Whether App Check enforcement is switched on for the project is a server-side setting that the binary does not show.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the project belongs to a health-records app and the bucket name sits in the same binary as the privacy text that says uploaded medical reports are stored server-side. The operator, not an outside observer, holds the evidence that the rules are correct (Art. 5(2)).

Impact: A Firebase project that belongs to an app handling health records can be reached with a key that every installed copy carries. Whether a third party can do more than consume quota depends on rules the operator has not shown.

Fix: Restrict the key by application signature and API, enforce App Check for the project, keep Storage and Auth rules at deny-by-default with per-user scoping, and publish the result of that review to the recipient of this notice.

M1: No operator identity, personal Gmail as privacy contact, legal address on another domain

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B)

The developer named on Google Play is Aivorn Technology and Consulting. That name appears nowhere in the binary, in the Privacy Policy, in the Terms or on the About page of medikhata.in. Those pages present the trading brand Medikhata with a city-level address in Mumbai, Maharashtra. No company suffix, no registration number and no governing-law clause appears in the Terms. The Privacy Office contact is a free Gmail address, although support@medikhata.in exists. libapp.so also contains legal@medikhata.com, a different domain from the app's own medikhata.in.

```
Privacy Policy page, schema.org Organization:
{"@type":"Organization","name":"Medikhata","url":"https://medikhata.in",
 "email":"support@medikhata.in","address":{"addressLocality":"Mumbai",
 "addressRegion":"Maharashtra","addressCountry":"IN"}}

Privacy Policy, Contact Us:
Medikhata Privacy Office
medikhataai@gmail.com

libapp.so string: legal@medikhata.com
```

Limits of this finding. A web search on 21 August 2026 showed that medikhata.com belongs to a product called MediKhata, Medical Practice Management for Doctors, which appears to be a different offering. Whether it is a sibling product, a rebrand remnant or an unrelated third party was not resolved.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because the missing controller identity blocks every data-subject right for users of a health-records app, and CVSS gives a pure transparency gap 0.0.

Impact: A user who wants to ask who holds a parent's lab history, or to have it deleted, finds a brand name and a private mailbox but no legal entity to address.

Fix: Name the legal entity, its registered address and its registration number in the in-app policy and on medikhata.in, publish a monitored privacy mailbox on the operator's own domain, and remove or explain the medikhata.com address.

M2: Play Data Safety lists health info for Analytics, against the FAQ

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B)

Google's Data Safety page, as declared by the developer, lists Health info as collected for App functionality, Analytics, Personalization and Account management, and Device or other IDs for Analytics. It lists Messages and Personal info (email address, phone number) as shared with other companies or organisations. It states that data is encrypted in transit. The FAQ claim that health data is stored on the device and never shared without consent does not fit this declaration.

```
Data shared (with other companies or organizations):
  Messages: Emails, SMS or MMS, Other in-app messages
    -> App functionality, Developer communications, Account management
  Personal info: Email address, Phone number
    -> App functionality, Account management

Data collected:
  Device or other IDs -> App functionality, Analytics, Account management
  Messages (Other in-app messages marked Optional)
    -> App functionality, Developer communications, Fraud prevention/security/
    compliance, Account management
  Files and docs -> App functionality
  Photos -> App functionality
  Health info -> App functionality, Analytics, Personalization, Account management
  Personal info (Name, Email address, Phone number, Other info)
    -> App functionality, Analytics, Developer communications,
       Fraud prevention/security/compliance, Personalization, Account management

Security practices: Data is encrypted in transit. You can request that data be deleted
    .
```

This is the developer's own declaration as Google renders it. It corroborates findings C1 and C2 and is listed separately because users read this label when they decide to install.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because the label is the first disclosure a prospective user sees and it concerns Art. 9 data. CVSS gives a pure disclosure inconsistency 0.0.

Impact: The label a person reads before installing describes broader use of health information than the FAQ inside the app, and names no recipient.

Fix: Align the Data Safety declaration, the in-app policy and the FAQ, and name the purposes for which health information is used.

M3: No Article 27 representative while installable in Austria

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B)

The Play listing for in.medikhata.app was fetched on 21 August 2026 with the footer Austria (English). The Play Store client on an Austrian-locale test device offered a normal install button for the app on the same date. An unrelated app on the same device showed a country-block message, so the client does surface restrictions when they exist. No Art. 27 representative is named in the binary, on medikhata.in or on the Play listing.

Whether Art. 3(2)(a) GDPR applies depends on whether the offer is directed at people in the Union. Installability in Austria and a listing without geographic restriction point that way. The marketing narrative, which RFI-IRFOS read as India-first with rupee currency and Indian emergency numbers, points the other way. RFI-IRFOS reports the facts and the question. It does not decide the question for the operator. The app was not installed.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because the app handles Art. 9 data and no EU contact exists at all. CVSS gives a representation gap 0.0.

Impact: If the offer is directed at the Union, an Austrian or other EU user of the app has no representative and no supervisory-authority contact other than the operator's own mailbox.

Fix: Name an Art. 27 representative or state in the listing and in the policy that the service is not offered in the Union, and restrict the Play distribution to match.

M4: Fine and coarse location permissions with no identified in-app feature

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.6 (CVSS-B)

ACCESS_FINE_LOCATION and ACCESS_COARSE_LOCATION are declared and a foreground GeolocatorLocationService is registered. A search of the extracted UI strings for nearby, nearest, pharmacy, hospital locator, find a doctor and current location found only the geolocator plugin's own permission strings. The marketing site mentions Indian emergency numbers (112, 102), which would need at most a country-level locale.

```
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
com.baseflow.geolocator.GeolocatorLocationService (manifest service)
```

Limits of this finding. A screen that string extraction did not capture could justify the permission. RFI-IRFOS raises a proportionality question for the operator and does not assert a violation.

Impact: A health-records app asks users for precise location and the operator has not said why.

Fix: Remove the permissions if no feature needs them, or document the feature and request the narrowest permission that serves it.

M5: One identity across three sign-in routes, no age handling for dependents

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B)

Phone (OTP), Google and Facebook sign-in all resolve through the same Firebase Auth identity, so the phone number or social token and the health records sit under one account. No date-of-birth minimum, parental-consent flow or age-differentiated logic was found for creating a family or dependent profile. The only date-of-birth string is the profile descriptor Profile details linked to health records (name, date of birth, gender). The About page describes a family use case.

```
com.google.firebase.auth.internal.GenericIdpActivity
com.google.firebase.auth.internal.RecaptchaActivity
com.facebook.FacebookActivity
com.facebook.CustomTabActivity  (scheme fbconnect, host cct.in.medikhata.app)
"Please enter your phone number to get verification code to continue"
api.medikhata.in/api/logs/log-otp-event
"Profile details linked to health records (name, date of birth, gender)"
```

Limits of this finding. Art. 8 concerns a child's own consent and may not apply if no minor registers. The gap examined here is the absence of any distinct handling when an adult enters a child's name, date of birth, gender and lab values as a dependent profile. A screen that string extraction did not capture could contain such handling.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because the data concerns children's health records, a group that merits specific protection under Recital 38, and no distinct handling was found. CVSS gives a design gap of this kind 0.0.

Impact: A parent can store a child's lab values in the same account and under the same rules as their own, and the child's data is subject to the same unnamed AI processor described in C1.

Fix: Add a dependent-profile flow that records the guardian relationship, applies age-appropriate handling and limits what leaves the device for minors.

Impact Analysis

The people affected are users who keep health records in the app: adults storing their own lab reports and prescriptions, and parents storing those of children and relatives through the family use case that the About page describes. The app is live on Google Play and installable on an Austrian account, so the group includes people in the Union.

What the evidence shows is a harm of opacity and default configuration. A user cannot learn from the app who receives uploaded health documents, because two screens give opposite answers and neither names a recipient (C1). SDKs from Google and Facebook handle identifiers from the first launch (C2, H1). The operator cannot be identified or addressed in a way that supports a data-subject request (M1, M3).

The analysis found no evidence that health content reached an advertising SDK, and it found no evidence of a breach or misuse. It did not examine the server side, so it does not say what the AI processor receives or retains.

The Complete Chain

Step 1, discovery and install: a user finds Medikhata on Google Play, reads the Data Safety label (M2) and installs the app. The developer field reads Aivorn Technology and Consulting (M1).

Step 2, first launch: Firebase and the Facebook SDK start as ContentProviders before any screen is shown (C2). The advertising identifier permission is present (H1).

Step 3, registration: the user signs in with phone, Google or Facebook and all three routes bind to one identity (M5). The app has no consent platform and shows no processor, controller or representative (C1, M1, M3).

Step 4, upload and chat: the user uploads a parent's or child's lab report or asks the AI chat a question. The client sends both to api.medikhata.in (C1).

Step 5, behind the backend: the privacy text says an AI processor analyses the report. The Help screen says nothing leaves the device. No document names the processor (C1).

Step 6, the user tries to act: the only functioning privacy contact is a Gmail mailbox. No entity and no EU representative can be addressed (M1, M3).

Child Protection & Dependent Profiles

The About page describes a family use case and the profile descriptor links name, date of birth and gender to health records. RFI-IRFOS found no flow that treats a child's profile differently from an adult's (M5). A child's lab values therefore sit under the parent's account with the same disclosures and the same processors as everyone else's data, including the AI analysis described in C1. Recital 38 GDPR asks for specific protection of children's data. Whether the operator has such handling in a screen that string extraction did not capture is a question the operator can answer.

Data Protection: Article by Article

Article 3(2) and Article 27: engaged by M3. Whether the offer is directed at people in the Union is open and depends on facts the operator knows. If it is, a representative is required and none is named.

Article 4(7) and Article 13(1)(a): engaged by M1. The controller is not identified in the app's own legal text.

Article 5(1)(a), Article 12(1) and Article 13(1)(e): engaged by C1, M1 and M2. The in-app texts contradict each other and no recipient of health data is named.

Article 5(1)(c): engaged by H1 and M4. The advertising identifier permission and the location permissions have no identified feature behind them.

Article 5(2): engaged by C2 and H2. The operator carries the burden of showing consent mechanisms and server-side rules.

Article 6(1), Article 7(1) and ePrivacy Directive Article 5(3): engaged by C2. Processing and access to terminal equipment begin before any consent mechanism exists.

Article 8: engaged conditionally by M5 for dependent profiles.

Article 9: engaged by C1, C2 and M5. Lab reports and prescriptions are health data and need an Art. 9(2) condition. The build shows none being obtained.

Article 25 and Article 32: engaged by H2. A project key and a bucket name ship in every install, and the safety of the project depends on settings the operator has not shown.

Article 44 and Article 46: engaged conditionally by C1. They apply if the unnamed AI processor sits outside the EEA.

Consumer Protection & Platform Disclosures

Three user-facing statements describe the same data in different ways: the Data Safety label on Google Play, the Privacy Policy screen and the FAQ. The FAQ says health data is stored on the device and never shared without consent. The label says health information is collected for Analytics and Personalization. The Privacy Policy screen says health data goes to processors for AI analysis. A consumer who relies on the first two statements is told something that the third contradicts.

The label says data is encrypted in transit, and the network security configuration blocks cleartext traffic, so that statement fits the build. Google Play publishes the label as the developer declares it. This report makes no statement about Google's own obligations.

Regulatory & Legal Landscape

No EU establishment of the controller was identified, so the one-stop-shop mechanism does not apply and the supervisory authority of each Member State where users are affected can act under Article 55. The Austrian Datenschutzbehörde and the European Data Protection Supervisor received the first notice in copy. The operator's FAQ refers to Indian data protection law, and RFI-IRFOS does not assess Indian law here.

The pre-consent initialisation pattern in C2 recurs across health and consumer apps in the RFI-IRFOS programme, which treats every operator under the same rules regardless of size. What sets this case apart is the combination with an in-app statement that data never leaves the device.

Indicators of Compromise & Reproducible Evidence

Every point below can be checked against the public Google Play build and the public web pages named.

```
Package         in.medikhata.app
Version         1.0.5 / versionCode 25 (updated on Google Play 2026-07-18)
Source          APKCombo mirror, base APK 25.8 MB, XAPK 84.5 MB
SHA-256         pending re-computation from the archived package before publication
Signing         generic Google distribution certificate (CN=Android, OU=Android, O=
    Google Inc.)
Min/target SDK  24 / 36
Developer       Aivorn Technology and Consulting (Google Play)
```

```
Firebase project   medikhata-auth
App ID             1:190353699967:android:5f5a462acb08dae151fb4a
Sender ID          190353699967
Storage bucket     medikhata-auth.firebasestorage.app
Facebook app ID    1841379369778337
API key and Facebook client token: present in res/values/strings.xml, values as
    extracted: AIzaSyB3aIcmPGjmqhOifIbAj8mlnNTdlOokfTo and facebook_client_token
    fc85a54585a420983480845d5ea0c667
```

```
api.medikhata.in    /api/chat /api/uploads /api/uploads/file/ /api/uploads/user/
                    /api/health/update/ /api/register /api/refresh-token
                    /api/logs/log-otp-event /api/notifications/toggle
Contact strings     medikhataai@gmail.com, support@medikhata.in, legal@medikhata.com
Pages read          medikhata.in/privacy, /terms, /about (2026-08-21)
Play pages          play.google.com/store/apps/details?id=in.medikhata.app
                    play.google.com/store/apps/datasafety?id=in.medikhata.app
    (2026-08-21)
```

```
grep -c on AndroidManifest.xml for FirebaseInitProvider, FacebookInitProvider
strings -n 6 libapp.so | grep -E "third-party processors|never shared without consent|
    stored securely on your device"
search of classes*.dex and libapp.so for OneTrust, Didomi, Usercentrics, IABTCF,
    consentmanager, cmpsdk: 0 matches
search for openai, gpt-, anthropic, generativelanguage, azure, cognitive, bedrock: 0
    matches
```

Disclosure Timeline & Outcome

2026-08-21 First notice (REF MEDIKHATA-2026-R1) to medikhataai@gmail.com and support@medikhata.in, CC dsb@dsb.gv.at and edps@edps.europa.eu, with three questions and a 14-day reply request.

2026-08-22 Delivery delay notice for support@medikhata.in.

2026-08-24 Second delay notice, then permanent failure for support@medikhata.in.

2026-09-04 The 14-day reply window closed with no answer.

2026-09-05 Follow-up to medikhataai@gmail.com restating the three questions.

2026-10-17 Reminder to medikhataai@gmail.com, 33 days before publication.

2026-11-14 No reply of any kind on the thread.

2026-11-19 Publication date, unchanged since the first notice.

What Medikhata Got Right

The network security configuration blocks cleartext traffic app-wide and explicitly for medikhata.in. The target SDK level is 36, which is current. A search for Tencent, ByteDance, Alibaba, Baidu, Mintegral, WeChat and Getui SDKs and for hardcoded .cn endpoints found nothing. There is no ad-mediation stack and no session-replay SDK. Local PDF rendering is present. The Data Retention section is specific, including a commitment that encrypted backups are purged within 30 days after deletion. Android backup is disabled.

Residual Risk & Recommendations

Everything in the findings table is open at the date of publication. A final APK diff before 19 November 2026 determines the state the published report records.

What remains unknown and matters most: the name and location of the AI processor, the legal basis for sending health data to it, the legal entity that is the controller, and whether the Firebase project's rules and App Check enforcement protect user data.

Recommendations: align the Privacy Policy screen, the FAQ and the Data Safety label and name every recipient of health data. Name the legal entity, its address and a monitored privacy mailbox on the operator's own domain. Appoint an Art. 27 representative or restrict distribution to match the intended market. Turn off automatic initialisation of Firebase Analytics and the Facebook SDK until a recorded consent choice exists. Remove the AD_ID and location permissions unless a feature needs them. Restrict the Firebase key, enforce App Check and keep Storage and Auth rules at deny-by-default. Add dependent-profile handling for children.

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 Root level code analysis of the published application

plus public web pages read by plain HTTP GET. No Medikhata server, key or account was used. Final report, published 21 November 2026. Coordinated disclosure under ISO/IEC 29147, Art. 17 StGG and GDPR Art. 89. RFI-IRFOS, ZVR 1015608684, GISA 39261441. REF MEDIKHATA-2026-R1.