Security & Privacy Disclosure, Final Report

Vivoo (app.vivoo.io)

A store label that says no data is shared, a policy that says the opposite, and no reply to three questions.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED 20 NOVEMBER 2026. NO REPLY OF ANY KIND AS OF 21 NOVEMBER 2026.

Target	Vivosens, Inc. (Vivoo)
Versions Audited	5.9.0 / 10107 (analysis 2026-08-21)
Notice / Publication	2026-08-22 / 2026-11-20 (90 days)
Findings	7: 1 High, 2 Medium, 2 Low, 2 observations (five disclosed severities reassessed in this report)
Status	NO REPLY OF ANY KIND AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`ed39afee5374dbc251d7c90d77900ae2e791d638a11a4a78ebd7bfee7d1ec0ac`

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 6

5 Engagement Summary 7

6 Findings 8
- 6.1 C1: Store label says no third-party sharing, policy and binary say otherwise . . 8
- 6.2 C2: Photos not listed as a collected data type, destination of the Meal Scan photo open 10
- 6.3 H1: Firebase API key and project identifiers hardcoded in strings.xml 11
- 6.4 H2: No age gate found in the dex files of an all-audiences app with pregnancy features 12
- 6.5 H3: Privacy policy names the Privacy Shield as a transfer mechanism 13
- 6.6 M1: No network security configuration and no certificate pinning 14
- 6.7 M2: RECORD_AUDIO listed without a purpose string 14

7 Impact Analysis 15

8 The Complete Chain 15

9 Consumer Protection & Platform Disclosures 16

10 Data Protection: Article by Article 16

11 Regulatory & Legal Landscape 17

12 Indicators of Compromise & Reproducible Evidence 17

13 Disclosure Timeline & Outcome 18

14 What Vivoo Got Right 18

15 Residual Risk & Recommendations 19

Executive Summary

Vivoo is a consumer wellness app from Vivosens, Inc., San Francisco. Users photograph urine test strips, and the app also covers pregnancy, fertility and menstrual cycle testing. On 22 August 2026 RFI-IRFOS sent a notice under REF VIVOO-2026-R1, based on a root level code analysis of version 5.9.0, to the support and developer addresses with the Datenschutzbehörde and the European Data Protection Supervisor in copy.

The lead finding is a contradiction between three documents. The Google Play Data Safety page says that no data is shared with third parties. The operator's own privacy policy says that information may be shared with third party companies for customer relations and advertising. The package contains Firebase, started by the operating system before any screen, plus CleverTap with its account ID and token in the manifest and Mixpanel, and no consent management platform at all. The people affected are users who log urinalysis results and, for some, pregnancy and fertility data. The report also records that the Data Safety list has no entry for photos, that the live policy names the Privacy Shield as a transfer mechanism more than six years after the Court of Justice invalidated it for the EU and US, and that the Firebase key and project identifiers are in the package.

Vivoo has not replied. The mailbox holds no answer, no automatic reply and no delivery failure notice for the notice, two follow-ups of 12 September and one follow-up of 17 October 2026. The three questions of the notice are open: which of the three sources is correct and on what legal basis the SDKs process data, where the Meal Scan photo goes, and what age check protects special-category data.

This report separates what the package shows from what only the operator can say. The strip scan runs on the device on the evidence of the package, and the destination of the Meal Scan photo is not shown. The logic of the app sits in a JavaScript bundle that was not disassembled. Compared with the notice, five severities are lower here, and one of them is recorded as an observation.

Scope: Root level code analysis of the Google Play release 5.9.0 (versionCode 10107) as an XAPK from a mirror, with the live Google Play Data Safety page and the live privacy policy read on 21 August 2026. Resources were decoded without sources and the dex files were searched for class names, endpoints and consent tokens. The Hermes JavaScript bundle was not disassembled. No application interface was queried, the Firebase key was not tested and no runtime instrumentation was used. The only network requests were the public assetlinks.json files of the two App Link hosts. No control flow analysis was performed. Where one would be needed the finding says UNVERIFIED.

ID	Severity	Title
C1	HIGH	Store label says no third-party sharing, policy and binary say otherwise
C2	LOW	Photos not listed as a collected data type, destination of the Meal Scan photo open
H1	MEDIUM	Firebase API key and project identifiers hardcoded in strings.xml
H2	INFO	No age gate found in the dex files of an all-audiences app with pregnancy features
H3	MEDIUM	Privacy policy names the Privacy Shield as a transfer mechanism
M1	LOW	No network security configuration and no certificate pinning
M2	INFO	RECORD_AUDIO listed without a purpose string

Finding Status at a Glance

The table shows the severity named in the notice of 22 August 2026 next to the severity in this report. Five labels differ. Every change follows from the evidence as described in the Basis column. No label changed because of a statement by Vivoo, which has not replied. M1 and M2 were first recorded in the full technical record and are shown as new.

ID	Notice	This report	Basis
C1	CRITICAL	HIGH	CVSS 6.9, raised one band by blast-radius escalation. Label, policy and SDK presence documented, data flow not observed.
C2	CRITICAL	LOW	CVSS 2.1. Strip photo processed locally, Meal Scan destination unverified.
H1	HIGH	MEDIUM	CVSS 6.3. Key exposure, Security Rules not examined.
H2	HIGH	INFO	Dex search cannot cover a JavaScript app, absence unverified.
H3	HIGH	MEDIUM	CVSS 6.3. Policy text documented, practice unverified.
M1	new	LOW	CVSS 2.3. Pinning absent, cleartext denied by default.
M2	new	INFO	Permission without purpose string, inference only.

Subject & Operator Analysis

Vivoo (package app.vivoo.io) is a consumer wellness app. Users photograph urine test strips with the phone camera and the app derives hydration, pH, ketone, magnesium, calcium, vitamin C and oxidative stress values. It also supports vaginal pH, LH, fertility and pregnancy strip tests, menstrual cycle logging, Health Connect body data sync, support for a Smart Toilet device over Bluetooth and a gallery photo Meal Scan nutrition feature.

The operator is Vivosens, Inc., 44 Tehama Street, Suite 409, San Francisco, CA 94105, USA. The same address appears in the app's Terms of Service, in Google Play's App support field and in the privacy policy. The Terms name California law and San Francisco County as venue. A different company, VivoSense, Inc. of Newport Coast, California, exists in medical device software and is not the operator. No data protection officer and no representative in the Union under Article 27 was found in the binary, the privacy policy, the Terms or the store listing, and both are UNVERIFIED. The app is listed on the Austrian Google Play store. The operator has no confirmed main establishment in the EU, so the one-stop-shop mechanism does not apply and each concerned authority is competent. For an Austrian matter that is the Datenschutzbehörde.

Item	Value
Package	app.vivoo.io
Version	5.9.0 (versionCode 10107), minSdk 29, targetSdk 36
base.apk SHA-256	ed39afee5374dbc251d7c90d77900ae2e791d638a11a4a78ebd7bfee7d1ec0ac
XAPK SHA-256	b1a47f1ea0e459e2ea8e0a55c0de1615c5d835b424560113317d7081af4119d0
Signer SHA-256	35:13:6F:89:EF:2F:69:29:5D:8F:DB:37:44:9D:59:52:31:D7:B9:66:91:49:00:59:DD:4A:82:BE:13:A6:54:91 (Google Play App Signing)
Size	XAPK 265.6 MB, base.apk 225,143,498 bytes
Code base	React Native with Expo, Hermes bytecode bundle assets/index.android.bundle (17.0 MB), 8 classes*.dex, native libraries including libonnxruntime.so, libVisionCamera.so, libreactnative.so, libzxingcpp_android.so
Source of the package	APKPure mirror. The app was absent from the audit device before the download. The manifest carries com.android.stamp.source = https://play.google.com/store and STAMP_TYPE_DISTRIBUTION_APK
Contacts	letstalk@vivoo.io (support, named in the Play listing and the privacy policy), hello@vivoo.io (developer contact in the Play listing). No privacy contact or DPO address found

Architecture & Data Flow

Resources were decoded without sources (apktool with no smali), and the dex files were copied raw and searched for SDK class names, endpoint strings and consent tokens. No control flow analysis was run. The Hermes JavaScript bundle could not be disassembled, and every statement that depends on logic that lives in the bundle is marked UNVERIFIED. The only network requests made during the analysis were two reads of the public assetlinks.json files of the two App Link hosts, which are static trust files. The application interface was not queried.

Layer	Observed	Source
Capture	Camera for the test strip, gallery picker for Meal Scan, Health Connect with a blocked list of sensitive record types, location and Bluetooth for a Smart Toilet device	assets/app.config, manifest
On-device analysis	Four ONNX Runtime models for strip and test detection, run by libonnxruntime.so	assets, native libraries
Analytics and marketing	CleverTap, Mixpanel, Sentry (org vivoo-eu), Firebase with Messaging	Manifest, dex
Backend hosts	asklepios.vivoo.io, api.vivoo.me (App Links, autoVerify), Firebase project vivoo-8cf55	Manifest, strings.xml
Updates	Expo over-the-air updates, so live JavaScript can differ from this package	Manifest
Consent	No consent management platform and no IAB TCF library	Dex search
Advertising	No ad mediation network found (no AppLovin, AdMob, Audience Network, Unity Ads, ironSource, InMobi, Vungle, Pangle or Mintegral)	Dex search

Engagement Summary

The notice went on 22 August 2026 at 05:58 UTC to letstalk@vivoo.io and hello@vivoo.io, with the Datenschutzbehörde and the European Data Protection Supervisor in copy. It named the findings C1 and C2 in full and summarised H1 to H3, set out three questions, asked for a reply within 14 days and for a named contact person, and gave the publication date of 20 November 2026. Two follow-ups went on 12 September 2026 and one on 17 October 2026. No message from Vivoo of any kind is in the mailbox as of 14 November 2026. No automatic reply and no delivery failure notice arrived for any of the four messages.

The thread offers no counterparty statement to assess. This report therefore records the status as no reply of any kind and makes no statement about the operator's position or internal handling.

Findings

C1: Store label says no third-party sharing, policy and binary say otherwise

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), editorial severity HIGH, disclosed as CRITICAL on 22 August 2026, re-assessed in this report

The Google Play Data Safety page of Vivoo, read on 21 August 2026, states: "No data shared with third parties. The developer says this app doesn't share user data with other companies or organizations." The operator's own privacy policy (vivoo.io/pages/privacy-policy, same date) states: "we may share your information with third party companies that work on behalf of our company for purposes such as customer relations, advertisement about goods and services which may interest you." The binary holds three integrated third-party SDKs: Firebase, started by a manifest ContentProvider before any screen can render, CleverTap with hardcoded account credentials, and Mixpanel. No consent management platform and no IAB TCF library appears in any of the 8 dex files. The package does not show what these SDKs transmit for a given user, and the JavaScript bundle that holds the CleverTap and Mixpanel initialisation calls was not disassembled, so their start time relative to any consent step is UNVERIFIED. The contradiction between label and policy is a documented fact that needs no runtime evidence. It was disclosed as CRITICAL on 22 August 2026 and is reassessed in this report to the band that the evidence supports. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the data comes from an app where users log urinalysis results and, for a subset, pregnancy, fertility and menstrual-cycle data, a category of health information that makes the same label contradiction weigh more than it would in an ordinary utility app.

```
No data shared with third parties
The developer says this app doesn't share user data with other companies or
    organizations.
```

```
<provider android:authorities="app.vivoo.io.firebaseinitprovider" android:
    directBootAware="true" and
    roid:exported="false" android:initOrder="100" android:name="com.google.firebase.
    provider.Firebas
    eInitProvider"/>
<meta-data android:name="CLEVERTAP_ACCOUNT_ID" android:value="6KK-8K8-Z46Z"/>
<meta-data android:name="CLEVERTAP_TOKEN" android:value="b3b-336"/>
```

```
com/clevertap  1,924 class hits  (marketing, CRM and push automation)
com/mixpanel     166 class hits  (product analytics)
io/sentry      1,684 class hits  (crash and performance, org vivoo-eu)
```

Android instantiates a manifest ContentProvider during application creation, before any Activity. FirebaseInitProvider also carries directBootAware, so it can run before the device is

unlocked. CleverTap and Mixpanel have no provider of their own in this manifest. Their initialisation sits in the Hermes JavaScript bundle (assets/index.android.bundle), which was not disassembled. The app also ships Expo over-the-air updates (expo.modules.updates.EXPO_UPDATE_URL), so the JavaScript on a live device can differ from the JavaScript in this package.

A consent-management search across all 8 dex files returned no hit for onetrust, didomi, usercentrics, consentmanager, iabtcf or IABTCF. The only TCF-like string, Landroidx/media3/extractor/text/cea/Cea708Decoder$DtvCcPacket, is a caption decoder token from the ExoPlayer library and not a consent framework. CleverTap ships an opt-out interface (setOptOut, getOptOutTracking, CLEVERTAP_OPTOUT). Its default state and whether the app exposes it to the user are UNVERIFIED.

Impact: People who log urinalysis results and, for some, pregnancy, fertility and cycle data read a store label that tells them no data is shared with other companies, while the operator's own policy says information may be shared with third party companies for customer relations and advertising.

Fix: State in writing which of the three sources is correct, name every third party that receives data from the app with its purpose and legal basis, correct the Data Safety label or the policy so that they agree, and place the initialisation of analytics and marketing SDKs behind a consent step.

C2: Photos not listed as a collected data type, destination of the Meal Scan photo open

LOW, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.1 (CVSS-B), disclosed as CRITICAL on 22 August 2026, reassessed in this report

Data Safety declares App activity, Health and fitness, Personal info, Location and App info and performance (crash logs). Photos is not in that list. Two photo access paths exist in the package. The first is a camera path for the test strip scan: android.permission.CAMERA, react-native-vision-camera (libVisionCamera.so) and the purpose string "Vivoo needs camera access to scan your test strip." It feeds four bundled on-device ONNX Runtime models and the bundled 18.3 MB libonnxruntime.so. All four are named for strip and test detection. The second is a gallery path for the Meal Scan feature: expo-image-picker with the purpose string "Allow Vivoo to access your photos to pick a meal image." None of the four models is named or shaped for food recognition. Whether the Meal Scan photo, or the raw strip photo, leaves the device is UNVERIFIED, because any upload call sits in the Hermes JavaScript bundle that was not disassembled and no network capture was made. The weight of the missing Photos entry depends entirely on that open question. It was disclosed as CRITICAL on 22 August 2026 and is reassessed in this report to the band that the evidence supports.

```
strip-model-v1-2-2.with_runtime_opt-2.ort        24 MB
multi-test-detection-v1-0-0.ort                  24 MB
ct-detection-1-1-0.with_runtime_opt.ort          24 MB
model-tiny.with_runtime_opt.ort                  24 MB
lib/armeabi-v7a/libonnxruntime.so                18,356,244 bytes
lib/armeabi-v7a/libonnxruntime4j_jni.so              55,056 bytes
```

```
"NSCameraUsageDescription": "Vivoo needs camera access to scan your test strip."
["expo-image-picker", { "photosPermission": "Allow Vivoo to access your photos to pick
     a meal image.
    " }]
```

The privacy policy mentions photographs or videos once, as marketing information obtained through surveys, contests and promotions. That sentence describes neither access path.

The strip photo of the core function is, on the evidence of the package, processed by local models. This is the design point recorded under What Vivoo Got Right. The unanswered part is the Meal Scan photo and the question of retention.

Impact: The people affected are users who photograph a body-derived test strip or a meal inside a health app. Whether either photo ever reaches a server cannot be read from the package.

Fix: Answer question 2 of the notice in writing: state whether the Meal Scan photo leaves the device, to which server and for how long it is kept, and align the Data Safety declaration with the answer.

H1: Firebase API key and project identifiers hardcoded in strings.xml

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N, 6.3 (CVSS-B), disclosed as HIGH on 22 August 2026, reassessed in this report

The values below ship in every copy of version 5.9.0. A Firebase API key in a client is expected and is not a secret by Google's design. A Realtime Database is provisioned for the project (firebase_database_url) and a Storage bucket is named. The notice described five abuse vectors: quota and billing exhaustion, unauthenticated Realtime Database read if the Security Rules are not deny-by-default, write access or data poisoning under the same misconfiguration, the absence of App Check as a multiplier, and the fact that a shipped key cannot be rotated for installed copies. The key was not tested against any server and the Security Rules were not examined, so only the first vector follows from the key alone. It was disclosed as HIGH on 22 August 2026 and is reassessed in this report to the band of its vector.

```
<string name="google_api_key">AIzaSyCKRxkpvfxNHSN-txoCl25gzPmPCgobCtc</string>
<string name="google_crash_reporting_api_key">AIzaSyCKRxkpvfxNHSN-txoCl25gzPmPCgobCtc
    </string>
<string name="firebase_database_url">https://vivoo-8cf55.firebaseio.com</string>
<string name="google_app_id">1:43826913203:android:46a8e68d43174a06</string>
<string name="google_storage_bucket">vivoo-8cf55.firebasestorage.app</string>
<string name="gcm_defaultSenderId">43826913203</string>
<string name="project_id">vivoo-8cf55</string>
<string name="default_web_client_id">43826913203-0i1k88h8qs741a29kfrhqu6npan2u71o.apps
    .googleusercon
    tent.com</string>
```

Impact: The direct exposure is the availability and billing of the operator's own Firebase project. Any exposure of user data would depend on the Security Rules, which are the operator's to confirm.

Fix: Restrict the key by package name and signing certificate, confirm deny-by-default Security Rules on the Realtime Database and the Storage bucket, and enforce App Check.

H2: No age gate found in the dex files of an all-audiences app with pregnancy features

INFO, no CVSS v4.0 score assigned, disclosed as HIGH on 22 August 2026, recorded as an observation

Google Play lists Vivoo with an all-audiences rating (PEGI 3, Everyone). The operator's description markets a women's health section with vaginal pH, LH, fertility and pregnancy urine tests and cycle logging. A search of all 8 dex files for age gate, age verification, COPPA, birth date collection and parental consent names returned no match beyond Android's own View.AUTOFILL_HINT_BIRTH_DATE constants. The application is written in React Native, and its screens and flows live in the Hermes JavaScript bundle, which was not disassembled. A dex search therefore cannot show whether an age screen exists in the JavaScript. The finding stands as the open question that the notice asked, and the absence itself is UNVERIFIED. It was disclosed as HIGH on 22 August 2026 and is recorded in this report as an observation for that reason.

```
Content rating on Google Play: PEGI 3 / Everyone
Dex search (8 files): age gate, age verification, COPPA, birthdate, parental consent:
    no match
Only hit: View.AUTOFILL_HINT_BIRTH_DATE_* (Android platform constants)
Not searched: assets/index.android.bundle (Hermes bytecode)
```

Impact: The question concerns whether a minor can reach pregnancy and fertility logging. The package cannot answer it.

Fix: Answer question 3 of the notice: state what age check exists before special-category data is processed, the basis under Article 8 where consent is used, and whether a data protection impact assessment exists.

H3: Privacy policy names the Privacy Shield as a transfer mechanism

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), disclosed as HIGH on 22 August 2026, reassessed in this report

The live privacy policy states, read on 21 August 2026: "We rely on multiple legal bases to lawfully transfer personal data around the world. These include your consent, the EU-US, and Swiss-US Privacy Shield, and the EU Commission approved model contractual clauses, which require certain privacy and security protections." The Court of Justice invalidated the EU-US Privacy Shield in Schrems II (Case C-311/18, 16 July 2020), so it is not a Chapter V transfer mechanism. The same sentence names standard contractual clauses, which remain a valid mechanism, so the policy does not say that the Privacy Shield is the only basis. The operator is a US company. Whether it relies on the Privacy Shield in practice, relies on the clauses, or is certified under a successor framework was not checked and is UNVERIFIED. The finding is the accuracy of the information that Article 13(1)(f) requires. It was disclosed as HIGH on 22 August 2026 and is reassessed in this report to the band that the evidence supports.

```
"We rely on multiple legal bases to lawfully transfer personal data around the world.
 These include your consent, the EU-US, and Swiss-US Privacy Shield, and the EU
    Commission
 approved model contractual clauses, which require certain privacy and security
    protections."
```

The Swiss-US Privacy Shield is named in the same sentence. This report relies on the invalidation of the EU-US framework, which is the one that concerns the GDPR, and does not assess the Swiss part.

Impact: A user who reads the policy to learn how data about their health leaves the EEA is told about a mechanism that has not been valid since July 2020.

Fix: Replace the sentence with the mechanism that the operator actually relies on for each transfer and state which processors receive the data.

M1: No network security configuration and no certificate pinning

LOW, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B)

The manifest declares no android:networkSecurityConfig and no usesCleartextTraffic, and res/xml holds no network_security_config.xml. Because targetSdkVersion is 36, the platform default denies cleartext traffic, which counts in the app's favour. The absence of any configuration also means that no certificate pinning exists for the two hosts that the manifest names (asklepios.vivoo.io and api.vivoo.me), so the TLS channel relies on the system trust store alone. A hostile certificate authority on a managed device would be the route to interception. The finding was first recorded in the full technical record and not in the body of the notice.

```
AndroidManifest.xml: no android:networkSecurityConfig, no usesCleartextTraffic
res/xml/: no network_security_config.xml
autoVerify App Link hosts: asklepios.vivoo.io, api.vivoo.me
```

Impact: The exposure is limited to a network attacker who controls a trusted certificate authority on the device. Health values travel over that channel.

Fix: Add pinning for the API hosts or document why system trust is accepted for this data.

M2: RECORD_AUDIO listed without a purpose string

INFO, no CVSS v4.0 score assigned, recorded as an observation

android.permission.RECORD_AUDIO is in the permissions array of assets/app.config. Every other dangerous permission in that file has a purpose string (camera, location, Bluetooth, photos, Health Connect). RECORD_AUDIO has none, and no microphone-related class or feature name was found in the dex string search. android.hardware.microphone is declared as not required. The most plausible explanation is a library default, for example the video recording path of react-native-vision-camera. That is an inference and not a confirmed call site, so the item is recorded as an observation. The finding was first recorded in the full technical record and not in the body of the notice.

```
"android.permission.ACCESS_COARSE_LOCATION", "android.permission.ACCESS_FINE_LOCATION
    ",
"android.permission.BLUETOOTH", "...", "android.permission.CAMERA", "...",
"android.permission.RECORD_AUDIO"
```

Impact: A microphone permission without a stated purpose leaves users unable to tell what it is for.

Fix: Remove the permission if no feature uses it, or add the purpose string.

Impact Analysis

Two groups of people stand in the path of the mechanisms in this report.

The first group is the users. They log urinalysis values and, for some, pregnancy, fertility and cycle data, under a store label that says no data is shared with other companies. The operator's own policy says information may be shared with third party companies for customer relations and advertising, and the package contains Firebase, CleverTap and Mixpanel. A user cannot tell from either text which companies receive what.

The second group is any user whose photos enter the app. The strip photo of the core function is processed on the device on the evidence of the package. The Meal Scan photo has no matching local model, and its destination is not shown.

This report does not claim that harm has occurred. It describes who stands in the path of each mechanism.

The Complete Chain

Step	Evidence	Finding
A person reads the store label and installs the app	Data Safety, read 21 Aug 2026	C1
Firebase starts before any screen, CleverTap and Mixpanel are integrated, no consent platform exists	Manifest, dex search	C1
The person photographs a strip or a meal	Camera and picker strings, ONNX models	C2
Pregnancy, fertility and cycle features are available without a found age check	Store description, dex search	H2
Data leaves the EEA under a policy that names a defunct mechanism	Policy text, read 21 Aug 2026	H3
The operator has not answered the three questions	Thread, 22 Aug to 17 Oct 2026	All

The weak link of the chain is the same in C1 and C2: the package shows which components exist, and only the operator can say what they receive.

Consumer Protection & Platform Disclosures

Google's Data Safety section is a statement by the developer about the developer's own app. For Vivoo it says no data is shared with third parties and lists five collected categories without Photos. The first statement is contradicted by the operator's own privacy policy in its own words, which is the strongest part of C1. Whether the missing Photos category breaches the platform's rules depends on whether the photos leave the device, and that is open.

The content rating is PEGI 3 / Everyone. The operator markets pregnancy and fertility testing. The rating assesses content, and the question of access by minors belongs to H2, which the package cannot settle.

The app is distributed through Google Play and the notice is addressed to the operator and not to the platform.

Data Protection: Article by Article

Article	Relevance	Finding
5(1)(a)	Transparency: label against policy against code	C1, C2
5(1)(c)	Minimisation: Meal Scan photo destination, microphone permission	C2, M2
6(1)	Legal basis for processing by Firebase, CleverTap and Mixpanel	C1
7(1)	Consent must precede processing, no consent platform found	C1
8	Age of consent for an information society service offered directly to a child, where consent is the basis	H2
9	Health, pregnancy and fertility data	C1, H2
13(1)(c), (e), (f)	Purposes, recipients and transfer information in the policy and the label	C1, C2, H3
25	Data protection by design: age assurance, provider initialisation	C1, H2
32(1)(a), (b)	Pinning, exposed Firebase key	M1, H1
35	Impact assessment for special-category processing	H2
44, 46	Transfer mechanism named in the policy	H3

Regulatory & Legal Landscape

The bases are Regulation (EU) 2016/679 (GDPR) with Articles 5, 6, 7, 8, 9, 13, 25, 32, 35, 44 and 46, and the Google Play Data Safety policy for the accuracy of developer declarations. The disclosure follows ISO/IEC 29147 and rests on the freedom of research under Article 17 of the Austrian Staatsgrundgesetz and Article 89 GDPR.

The operator is established in the United States. The Austrian Google Play listing indicates that the app is offered to people in the Union, which would bring Article 3(2) and the duty to designate a representative under Article 27 into play. That applicability was not established and the representative was not found. Without a main establishment in the Union, each concerned authority is competent. The Datenschutzbehörde (dsb@dsb.gv.at) and the European Data Protection Supervisor (edps@edps.europa.eu) were in copy of the notice of 22 August 2026 and of the second follow-up of 12 September 2026.

The report makes no comparison with other applications.

Indicators of Compromise & Reproducible Evidence

Every item can be reproduced from the package named below. The Firebase key was not tested and no account was created.

```
Package       app.vivoo.io 5.9.0 (10107)
base.apk      ed39afee5374dbc251d7c90d77900ae2e791d638a11a4a78ebd7bfee7d1ec0ac
XAPK          b1a47f1ea0e459e2ea8e0a55c0de1615c5d835b424560113317d7081af4119d0
Signer        35:13:6F:89:EF:2F:69:29:5D:8F:DB:37:44:9D:59:52:31:D7:B9:66:91:49:00:59:
    DD:4A:82:BE:13
    :A6:54:91
Firebase      vivoo-8cf55, https://vivoo-8cf55.firebaseio.com, vivoo-8cf55.
    firebasestorage.app
API key       AIzaSyCKRxkpvfxNHSN-txoCl25gzPmPCgobCtc
App ID        1:43826913203:android:46a8e68d43174a06, sender 43826913203
Web client    43826913203-0i1k88h8qs741a29kfrhqu6npan2u71o.apps.googleusercontent.com
CleverTap     account ID 6KK-8K8-Z46Z, token b3b-336
Provider      app.vivoo.io.firebaseinitprovider (initOrder 100, directBootAware)
Models        strip-model-v1-2-2.with_runtime_opt-2.ort, multi-test-detection-v1-0-0.
    ort,
              ct-detection-1-1-0.with_runtime_opt.ort, model-tiny.with_runtime_opt.ort
Hosts         asklepios.vivoo.io, api.vivoo.me
Policy        https://www.vivoo.io/pages/privacy-policy
Contacts      letstalk@vivoo.io, hello@vivoo.io
```

The full values of all identifiers are given in clear text as they appear in the package.

Disclosure Timeline & Outcome

Date	Event
22 Aug 2026	Notice REF VIVOO-2026-R1 at 05:58 UTC to letstalk@vivoo.io and hello@vivoo.io, Datenschutzbehörde and EDPS in copy. C1 and C2 in full, H1 to H3 summarised, three questions, reply requested within 14 days, publication stated as 20 November 2026.
12 Sep 2026	13:31 UTC first follow-up: no reply of any kind after 21 days, C1 and C2 restated, the three questions repeated, answer requested by 19 September 2026. 17:07 UTC second message in the older thread subject, Datenschutzbehörde and EDPS in copy, with the open points and the Privacy Shield question.
17 Oct 2026	Follow-up 34 days before publication, 56 days after the notice, to both addresses.
14 Nov 2026	No message from Vivoo. No automatic reply and no delivery failure notice for any of the four messages.
20 Nov 2026	Publication date, unchanged since 22 August 2026.

Outcome as of 14 November 2026: no reply of any kind, no answer to any of the three questions, no named contact person.

What Vivoo Got Right

The core strip scan runs on the device through four ONNX Runtime models, with no cloud vision SDK found anywhere in that path. That is a better design than uploading strip photos for analysis, and the evidence supports it for the strip scan only.

The Health Connect integration blocks permissions for blood glucose, blood pressure, body fat, body temperature, respiratory rate, resting heart rate, heart rate variability, lean body mass and VO2 max (blockedPermissions in assets/app.config), a concrete decision to request less than the platform allows. allowBackup is false. targetSdkVersion is 36, so cleartext traffic is denied by default. The two App Link hosts serve assetlinks.json files whose certificate fingerprint matches the app’s own signing certificate, which rules out a deep link hijack for both hosts. The package is a genuine Google Play distribution build and not a repackage. No ad mediation network was found. CleverTap’s opt-out interface is present in the code.

Residual Risk & Recommendations

Priority	Action	Finding
1	Say which of label, policy and code is correct and list every third party that receives data, with purpose and legal basis	C1
2	Move the start of analytics and marketing SDKs behind a consent step	C1
3	State where the Meal Scan photo goes and how long it is kept, then align the Data Safety declaration	C2
4	Replace the Privacy Shield sentence with the actual transfer mechanism	H3
5	Describe the age check before special-category data is processed	H2
6	Restrict the Firebase key, confirm deny-by-default rules, enforce App Check	H1
7	Pin the API hosts and remove the unused microphone permission	M1, M2

Residual risk: the Hermes JavaScript bundle holds the logic behind C1, C2 and H2 and was not disassembled. A later build can differ because Expo over-the-air updates are enabled. This report describes version 5.9.0 only. The open questions are the three questions of the notice, and they stay open until the operator answers them.

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 the live Google Play Data Safety page and privacy policy. The Firebase key was not tested and the application interface was not queried. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Arts. 5, 6, 7, 8, 9, 13, 25, 32, 35, 44, 46. RFI-IRFOS ZVR 1015608684, GISA 39261441. REF VIVOO-2026-R1.