Security & Privacy Disclosure, Final Report

YO Home Sperm Test (com.mes.YO_3_0.official_yo_3_0)

A semen test app with a cleartext video link, a store label that says no sharing, and automatic acknowledgements in place of answers.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. EMBARGO 20 NOVEMBER 2026. ONLY AUTOMATED ACKNOWLEDGEMENTS, NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026.

Target	Medical Electronic Systems (LLC, Encino, and Limited, Caesarea)
Versions Audited	257.0.5.1 / 576 (analysis 2026-08-22)
Notice / Publication	2026-08-22 / 2026-11-20 (90 days, unchanged); final report published 2026-11-21
Findings	11: 1 High, 5 Medium, 2 Low, 3 observations (ten disclosed severities reassessed in this report)
Status	ONLY AUTOMATED ACKNOWLEDGEMENTS, NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026. Four messages sent, four automatic ticket receipts.
SHA-256 (base APK)	`d0d8e3a52fc2c0150f2fa8fc58d8c0f3cee689e4f20ec8426f6235156e974fcb`

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: Cleartext HTTP and RTSP allowed to the test device's WiFi address 8
- 6.2 C2: Sample video analysed in the cloud, a development analysis endpoint ships in the app 9
- 6.3 C3: Firebase starts before the onboarding acceptance screens can render . . 10
- 6.4 C4: Store label says no third-party sharing, policy and compiled SDK say otherwise 11
- 6.5 H1: Fine and background location requested, policy names a second purpose 12
- 6.6 H2: Partner's ovulation tracking status stored on the account holder's profile . 13
- 6.7 H3: No certificate pinning configured for any endpoint 14
- 6.8 M1: Google API key hardcoded, four cloud project references in one app . . . 15
- 6.9 H4: Policy requires age 18, Play rating is PEGI 3, onboarding strings show no age step 16
- 6.10 M2: Marketing messages tied to account creation 16
- 6.11 M3: Two legal entities named as operator, no EU representative named 17

7 Impact Analysis 17

8 The Complete Chain 18

9 Inference Data, Bystanders and Control 18

10 Consumer Protection & Platform Disclosures 19

11 Data Protection: Article by Article 19

12 Regulatory & Legal Landscape 20

13 Indicators of Compromise & Reproducible Evidence 20

14 Disclosure Timeline & Outcome 21

15 What the Operator Got Right 21

16 Residual Risk & Recommendations 22

Executive Summary

YO Home Sperm Test is the companion app for a Class II over-the-counter home semen analysis device from Medical Electronic Systems. The app connects to the device's own WiFi, plays the sample video and shows results computed by a cloud service. On 22 August 2026 RFI-IRFOS sent a notice under REF YOHOMESPERMTEST-2026-R1, based on a root level code analysis of version 257.0.5.1, to the support and developer addresses with the Datenschutzbehörde and the European Data Protection Supervisor in copy.

The lead finding is a contradiction between the store label and the operator's own documents. The Google Play Data Safety section says that no data is shared with third parties. The privacy policy names Firebase, BigQuery and Co-pilot CX Ltd and says that email and name may go to affiliates for marketing. The package holds a Co-pilot CX class hierarchy that handles login, signup and password reset. The report also records a network configuration that allows cleartext HTTP and RTSP to the device's WiFi address, a development analysis endpoint inside the production app, Firebase starting before the acceptance screens, a stored attribute about the user's partner, and a mismatch between the policy's age limit of 18 and the rating PEGI 3.

The operator has not replied substantively. Its support system sent an automatic acknowledgement for each of the four messages of this case, tickets 27089, 27375, 27895 and 28228, and nothing else arrived by 21 November 2026. An automatic acknowledgement is not an answer to the findings. The three questions of the notice are open: what protects the sample video in transit, which of label and policy is correct, and what keeps minors out. The embargo date of 20 November 2026 has passed, and this final report is published on 21 November 2026.

This report separates what the package shows from what only the operator can say. The video transport is inferred from the configuration and was not captured, and the Dart code that holds the logic was not disassembled. Compared with the notice, ten severities are lower here and three items are recorded as observations.

Scope: Root level code analysis of the Google Play release 257.0.5.1 (versionCode 576) as an XAPK from a mirror, with the live Google Play listing and the privacy policy read on 22 August 2026. Resources were decoded without sources, and the dex files and libapp.so were searched with strings and grep. The Dart snapshot was not disassembled. No endpoint was called, the Google key was not tested, no traffic was captured and no runtime instrumentation was used. No control flow analysis was performed. Where one would be needed the finding says UNVERIFIED.

ID	Severity	Title
C1	MEDIUM	Cleartext HTTP and RTSP allowed to the test device's WiFi address
C2	MEDIUM	Sample video analysed in the cloud, a development analysis endpoint ships in the app
C3	MEDIUM	Firebase starts before the onboarding acceptance screens can render
C4	HIGH	Store label says no third-party sharing, policy and compiled SDK say otherwise
H1	LOW	Fine and background location requested, policy names a second purpose
H2	MEDIUM	Partner's ovulation tracking status stored on the account holder's profile
H3	LOW	No certificate pinning configured for any endpoint
M1	MEDIUM	Google API key hardcoded, four cloud project references in one app
H4	INFO	Policy requires age 18, Play rating is PEGI 3, onboarding strings show no age step
M2	INFO	Marketing messages tied to account creation
M3	INFO	Two legal entities named as operator, no EU representative named

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. Ten labels differ. Every change follows from the evidence as described in the Basis column. No label changed because of a statement by the operator, which has not replied substantively.

ID	Notice	This report	Basis
C1	CRITICAL	MEDIUM	CVSS 6.0. Cleartext exception documented, transport content inferred, local network only.
C2	CRITICAL	MEDIUM	CVSS 6.3. Endpoint reference documented, no endpoint tested.
C3	CRITICAL	MEDIUM	CVSS 6.9. Structural sequence documented, data flow not observed.
C4	CRITICAL	HIGH	CVSS 6.9, raised one band by blast-radius escalation. Label, policy and SDK documented.
H1	HIGH	LOW	CVSS 2.1. Permissions and policy text documented, background use not observed.
H2	HIGH	MEDIUM	CVSS 2.1, raised one band by blast-radius escalation. Field documented, storage not observed.

ID	Notice	This report	Basis
H3	HIGH	LOW	CVSS 2.3. Pinning absent, system trust in effect.
H4	HIGH	INFO	Mismatch documented, absence of an age step drawn from strings.
M1	MEDIUM	MEDIUM	CVSS 6.3. Key exposure, rules not examined.
M2	MEDIUM	INFO	Policy wording, no technical score.
M3	MEDIUM	INFO	Naming difference documented, no technical score.

Subject & Operator Analysis

YO Home Sperm Test (package com.mes.YO_3_0.official_yo_3_0, app label YO Home Test in the binary) is the companion app for the YO Testing Device, a Class II over-the-counter home semen analysis device. The Play listing shows 10,000+ downloads, rating PEGI 3 and the category Medical. The phone's camera is not used. The device creates its own WiFi access point, and the app connects to it and plays a video stream through the media_kit plugin. The video is analysed by a cloud service, and the app presents derived values such as concentration and motility.

Two legal entities appear. The Play listing names Medical Electronic Systems, LLC of Encino, California. The privacy policy names Medical Electronic Systems Limited of Caesarea Industrial Park, Israel as the GDPR controller and a data protection officer, Taly Vider Cohen, reachable through support@yospermtest.com. No representative in the Union is named in either document. Neither entity has a disclosed main establishment in the Union, so each concerned authority is competent, and for an Austrian matter that is the Datenschutzbehörde.

Item	Value
Package	com.mes.YO_3_0.official_yo_3_0
Version	257.0.5.1 (versionCode 576), minSdk 24, targetSdk 36
XAPK SHA-256	c909b2e3ecbf4e2152389d4feefcb561ee5c48012c5debf34add7289daf71c2e
base.apk SHA-256	d0d8e3a52fc2c0150f2fa8fc58d8c0f3cee689e4f20ec8426f6235156e974fcb
config.arm64_v8a.apk SHA-256	2d6da8d9bd36452984c209fda87e62b4ef1b18313c958d876e0f1a8db16e7f8d
Size	XAPK 53 MB (base 16 MB, arm64 split 37 MB, 18 language and density splits)
Code base	Flutter and Dart, logic AOT-compiled in libapp.so. 24,439 class definitions in 6 dex files, counted from the dex headers. libmpv.so and libmediakitandroidhelper.so for video
Source of the package	APKPure mirror, version and developer cross-checked against the live Play listing. The audit device was not connected for this run

Item	Value
Contacts	support@yospermtest.com (support, Play listing and privacy policy), itay@mes-ltd.com (developer contact, Play listing)

Architecture & Data Flow

Resources were decoded without sources (apktool with no smali). The dex files and the unpacked libapp.so were searched with strings and grep. No baksmali, no jadx and no Dart disassembly was run, so the logic of the app is not readable at source level and any finding that needs code path tracing is marked UNVERIFIED. No dynamic instrumentation and no live backend call was made.

Layer	Observed	Source
Device link	Cleartext HTTP and RTSP allowed to 192.168.0.1, libmpv.so, no camera permission	network_security_config.xml, manifest
Analysis	No bundled model, /analyzevideo route, four cloud endpoints including a development one	libapp.so
Accounts	Login, signup and password reset through Co-pilot CX (com.copilot.authentication)	Dex, libapp.so
Analytics	Firebase with Analytics and Crashlytics, BigQuery named in the policy, Co-pilot analytics	Manifest, dex, policy
Location	Fine, coarse and background location	Manifest
Profile	Age, partner ovulation tracking status	Translations, libapp.so
Other permissions	Calendar read and write for a single next-test reminder, biometric login, notifications, exact alarms, phone state, storage, WRITE_SETTINGS	Manifest
Not requested	CAMERA, RECORD_AUDIO, Bluetooth, READ_CONTACTS. No notification listener service	Manifest, dex

Engagement Summary

The notice went on 22 August 2026 at 17:10 UTC to support@yospermtest.com and itay@mes-ltd.com, with the Datenschutzbehörde and the European Data Protection Supervisor in copy. It named eleven findings, four of them critical, set out three questions and stated publication on 20 November 2026. The operator's support system answered each of the four messages that this case sent (22 August, 12 September, 17 October and 15 November 2026) with an automatic acknowledgement and a ticket number: 27089 on 22 August 2026 at 17:11 UTC, 27375 on 12 September 2026 at 16:32 UTC, 27895 on 18 October 2026 at 19:22 UTC and 28228 on 15 November 2026 at 12:59 UTC. Each says that the request has been received and is being reviewed by support staff.

The mailbox holds no message from the operator beyond these four acknowledgements, no answer to any of the three questions and no delivery failure notice. An automatic acknowledgement is not a response to the findings. This report records the status as no substantive reply.

Findings

C1: Cleartext HTTP and RTSP allowed to the test device's WiFi address

MEDIUM, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.0 (CVSS-B), disclosed as CRITICAL on 22 August 2026, reassessed in this report

res/xml/network_security_config.xml permits cleartext HTTP and RTSP traffic to exactly one address, 192.168.0.1, which is the address of the YO Testing Device's own WiFi access point. The application default (android:usesCleartextTraffic="false") blocks cleartext everywhere else. The package bundles libmpv.so (12.4 MB, the mpv media player engine) and libmediakitandroidhelper.so through the Flutter media_kit plugin, which is a video playback stack and not a still image library. The manifest declares no android.permission.CAMERA and no camera hardware feature, so the phone's own camera is not used. The location permission dialog says the app needs location to "establish a direct WiFi connection" to the device, and the interface copy narrates a recording step ("Video Now Recording"). Read together, the configuration is consistent with a design in which the microscopy video of the sample travels from the device to the phone without transport encryption. That reading is an inference. No packet was captured and no test was run. An attacker would have to be on the device's own short-lived WiFi network during a test. It was disclosed as CRITICAL on 22 August 2026 and is reassessed in this report to the band that the evidence supports.

```
<network-security-config>
    <domain-config cleartextTrafficPermitted="true">
        <domain includeSubdomains="true">http://192.168.0.1</domain>
        <domain includeSubdomains="true">rtsp://192.168.0.1</domain>
    </domain-config>
</network-security-config>
```

```
dialog.popup.location_permission_required.body => The YO App needs your location
    permission to run t
    he test.
Location Services are used to confirm that your phone is close enough to the YO device
     so that other
     WiFi networks do not interfere with your test.
Please allow the YO App to connect to your phone and establish a direct WiFi
    connection.
test_flow.video_now_recording => "Video Now Recording"
```

The cleartext exception is narrow: one local address, nothing public. The sensitivity of the content, if the stream is the sample video, is high, which is why the confidentiality impact is rated high in the vector and the attack conditions are rated demanding.

Impact: The people affected are users of a home semen analysis device. If the stream is the sample video, a person on the same short-lived device network during a test could read it.

Fix: Answer question 1 of the notice in writing: state what protects the video in transit over the local link if not transport encryption.

C2: Sample video analysed in the cloud, a development analysis endpoint ships in the app

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 CRITICAL on 22 August 2026, reassessed in this report

No .tflite, .onnx or other model file exists in the package, so the analysis is not on the device. The Dart source paths kept in the compiled libapp.so name the pipeline (yo_analyzing_api.dart, yo_data_center_api.dart, analyzing_repository.dart, analyze_results_model.dart) and an /analyzevideo route. Four Google Cloud endpoints are hard-coded, among them yo-dev-analysis-wucicmh3qa-uc.a.run.app next to the production yoanalysis-wucicmh3qa-uc.a.run.app. A development or staging instance of the service that computes fertility results from biological video is referenced by the build that every user downloads. No call was made to any endpoint, so its authentication, logging and reachability are UNVERIFIED. The finding is that the reference ships. It was disclosed as CRITICAL on 22 August 2026 and is reassessed in this report to the band that the evidence supports.

```
package:official_yo_3_0/analyze/data/dataProviders/yo_analyzing_api.dart
package:official_yo_3_0/analyze/data/dataProviders/yo_data_center_api.dart
package:official_yo_3_0/analyze/data/repositories/analyzing_repository.dart
package:official_yo_3_0/analyze/data/models/analyze_results_model.dart
/analyzevideo
```

```
https://us-central1-yodatacenter.cloudfunctions.net
https://us-central1-yohome-2019.cloudfunctions.net
https://yoanalysis-wucicmh3qa-uc.a.run.app
https://yo-dev-analysis-wucicmh3qa-uc.a.run.app
```

Impact: The people affected are users whose sample video is processed by a cloud service. A development instance of that service is named in the app they install.

Fix: Remove the development endpoint from production builds and state how the production analysis service authenticates the app.

C3: Firebase starts before the onboarding acceptance screens can render

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), disclosed as CRITICAL on 22 August 2026, reassessed in this report

FirebaseInitProvider is declared with directBootAware="true" and initOrder="100", next to AppMeasurementService and AppMeasurementReceiver. Android instantiates a manifest ContentProvider during application creation, before any Activity. The onboarding copy says: "By selecting \"I Accept\", you agree that you have read and understand the terms of our Privacy Policy and expressly authorize YO App to use your health data as set forth in the data privacy policy." Firebase measurement and crash processing can therefore begin before the screen that this sentence belongs to can appear. What Firebase transmits was not observed. It was disclosed as CRITICAL on 22 August 2026 and is reassessed in this report to the band that the evidence supports.

```
<provider android:authorities="com.mes.YO_3_0.official_yo_3_0.firebaseinitprovider"
    android:directBo
    otAware="true" android:exported="false" android:initOrder="100" android:name="com.
    google.firebas
    e.provider.FirebaseInitProvider"/>
<service android:enabled="true" android:exported="false" android:name="com.google.
    android.gms.measur
    ement.AppMeasurementService"/>
<receiver android:enabled="true" android:exported="false" android:name="com.google.
    android.gms.measu
    rement.AppMeasurementReceiver"/>
```

```
onboarding.screens.terms_of_service.body_2 => By selecting 'I Accept', you agree to
    the Terms of Ser
    vice and Use.
onboarding.screens.data_privacy_policy.body_3 => By selecting "I Accept", you agree
    that you have re
    ad and understand the terms of our Privacy Policy and expressly authorize YO App
    to use your hea
    lth data as set forth in the data privacy policy.
```

The package also declares com.google.android.gms.permission.AD_ID, ACCESS_ADSERVICES_ATTRIBUTION and ACCESS_ADSERVICES_AD_ID, and the install referrer binding. No display ad SDK exists in the package. The permissions fit Firebase's own install attribution and are folded into this finding and not rated separately.

Impact: The people affected are users who are told that acceptance is the trigger for data use, in an app where the analytics component starts earlier.

Fix: Start Firebase measurement and crash reporting only after the acceptance step, or document the legal basis on which they run earlier.

C4: Store label says no third-party sharing, policy and compiled SDK 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 section, read on 22 August 2026, says: "No data shared with third parties. This app may collect these data types: Personal info, Health and fitness, and Messages. Data is encrypted in transit. You can request that data be deleted." The privacy policy linked inside the app says: "Your information is securely stored in Firebase and Bigquery. We store the data on secure cloud services running in the United States." It names "Co-pilot CX Ltd to analyze patterns of usage to improve the customer experience" and states: "We many share your personal data (but not health-related information) with carefully selected third parties for marketing purposes. For example, we are allowed to share your email and name with our affiliates who could then use these to offer promotions to you." The dex files hold a com.copilot.authentication and com.copilot.analytics class hierarchy, and libapp.so holds the Dart paths auth_copilot_repository.dart and copilot_user_model.dart, so the login, signup and password reset of the app's accounts are delegated to a named external provider. The endpoint sphere.bycopilot.com/v2/partner/{partnerId}/acquire_ticket is in the dex strings. Whether a data processing agreement exists with that provider is not shown by the package. The contradiction between label and policy is a documented fact. 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 label contradiction concerns an app for reproductive health testing whose account login is delegated to a named external provider, a category of health information that makes the contradiction weigh more than it would in an ordinary utility app.

```
No data shared with third parties
This app may collect these data types: Personal info, Health and fitness, and Messages
    .
Data is encrypted in transit. You can request that data be deleted.
```

```
Lcom/copilot/authentication/interfaces/TokenProvider;
Lcom/copilot/authentication/model/enums/LoginError;
Lcom/copilot/authentication/model/enums/LoginSilentlyError;
Lcom/copilot/authentication/model/enums/LogoutError;
Lcom/copilot/authentication/model/enums/ResetPasswordError;
Lcom/copilot/authentication/model/enums/SignupError;
Lcom/copilot/analytics/AbstractAnalyticsEvent;
Lcom/copilot/analytics/CustomAnalyticsEvent;
Lcom/copilot/analytics/EventLogProvider;
sphere.bycopilot.com/v2/partner/{partnerId}/acquire_ticket
```

```
package:official_yo_3_0/authentication/data/repositories/auth_copilot_repository.dart
package:official_yo_3_0/authentication/data/models/copilot_user_model.dart
```

Impact: People who test their semen quality with a home device read a store label that says

no data is shared with third parties, while the operator's own policy names Firebase, BigQuery, Co-pilot CX Ltd and affiliates that receive email and name for marketing.

Fix: State which of label and policy is correct, confirm whether an Article 28 agreement exists with the authentication provider, and correct the Data Safety label.

H1: Fine and background location requested, policy names a second purpose

---

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

The manifest requests ACCESS_FINE_LOCATION, ACCESS_BACKGROUND_LOCATION and ACCESS_COARSE_LOCATION. The only purpose shown in the app is the WiFi proximity check quoted under C1. A foreground WiFi scan does not need background location, which grants access while the app is not in use. The privacy policy names a second purpose that the in-app dialog does not: "Geo-location data, we use this data to establish a WiFi connection and suggest physicians in your proximity." It also describes the data as "approximate location data", which does not match the permission scope requested. Whether the app reads location in the background was not observed. It was disclosed as HIGH on 22 August 2026 and is reassessed in this report to the band of its vector.

```
android.permission.ACCESS_FINE_LOCATION
android.permission.ACCESS_BACKGROUND_LOCATION
android.permission.ACCESS_COARSE_LOCATION
```

```
Geo-location data - we use this data to establish a WiFi connection and suggest
    physicians in your p
    roximity.
Contact Data: includes approximate location data, email address, wi-fi name, internet
    connection det
    ails, connection speed.
```

Impact: Users of a fertility testing device are asked for a location permission whose in-app reason is narrower than the policy's.

Fix: Remove the background location permission if no feature needs it and state the physician suggestion purpose where the permission is requested.

H2: Partner’s ovulation tracking status stored on the account holder’s profile

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

The settings of the app include an input named SettingsIsPartnerTrackingOvulationInput (settings_is_partner_tracking_ovulation_input.dart, field isPartnerTrackingOvulation) with the question ”Is your partner testing or tracking their ovulation?” The field describes a person who never installed the app, never saw its Terms of Service and never accepted its Data Privacy Policy. Next to the account holder’s own semen analysis results, it allows a fertility profile of a couple to form on one account. The package shows the field and its wording. Whether the value is sent to a server was not observed. RFI-IRFOS blast-radius escalation: raised from LOW/2.1 to MEDIUM because the person described never installed the app and never saw a notice, and the attribute is a person’s reproductive health tracking status.

```
package:official_yo_3_0/settings/widgets/inputs/
    settings_is_partner_tracking_ovulation_input.dart
SettingsIsPartnerTrackingOvulationInput
isPartnerTrackingOvulation
```

```
settings.user_data.is_partner_tracking_ovulation.title => Partner Testing or Tracking
    Ovulation
settings.user_data.is_partner_tracking_ovulation.question => Is your partner testing
    or tracking the
    ir ovulation?
```

Impact: The person described is the partner of a user. The partner has no notice, no consent screen and no relationship with the operator, and the attribute concerns reproductive health.

Fix: State where the partner field is stored, on what basis the data about the partner is processed and how the partner is informed.

H3: No certificate pinning configured for any endpoint

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), disclosed as HIGH on 22 August 2026, reassessed in this report

The whole network_security_config.xml is the single domain-config block shown under C1. No pin-set exists for any domain, including the Google Cloud and Firebase hosts (*.googleapis.com, *.cloudfunctions.net, *.run.app) that carry account credentials and analysis results once the video leaves the local link. The bundled OkHttp library has a CertificatePinner class, which is a library capability and not a configured pin. No pin value was found in the manifest, the resources or the extracted strings. System trust store TLS remains in effect. It was disclosed as HIGH on 22 August 2026 and is re-assessed in this report to the band of its vector.

```
res/xml/network_security_config.xml: one domain-config block, no pin-set element
okhttp3.CertificatePinner present as library class, no pin values found
```

Impact: The exposure is limited to a network attacker who controls a trusted certificate authority on the device.

Fix: Add pinning for the operator’s cloud hosts or document why system trust is accepted for this data.

M1: Google API key hardcoded, four cloud project references in one app

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)

res/values/strings.xml holds a Google API key, identical for google_api_key and google_crash_reporting_api_key, with the project yo-home-sperm-test, a sender ID, an app ID and a Cloud Storage bucket. The values are given as quoted in the notice of 22 August 2026. A Cloud Firestore client is used throughout the compiled Dart code. A Firebase key in a client is expected and is not a secret by Google's design. The notice described five vectors: calling /analyzevideo and the other endpoints of C2 directly, Firestore access if the rules are not scoped, an open storage bucket acting as a file server, project enumeration from the key, and the fact that a shipped key cannot be rotated for installed copies. The key was not tested and no rules were examined, so only exposure of the operator's own project to quota abuse follows from the key alone. In addition, the package refers to four different cloud projects: yo-home-sperm-test in strings.xml, and yodatacenter, yohome-2019 and the yoanalysis pair in libapp.so. Which of them are live, retired or aliased was not determined. The sprawl is a transparency point, because a person who files an access request cannot tell how many systems their data touched.

```
project_id: yo-home-sperm-test
google_storage_bucket: yo-home-sperm-test.appspot.com
google_api_key = google_crash_reporting_api_key:
    AIzaSyCpYg8w4so7r5H2qL3QJ7ozHf8rTI3rbc4
gcm_defaultSenderId: 377022562223
google_app_id: 1:377022562223:android:7fc0b787961d18f88fb95a
```

Impact: The direct exposure is the availability and billing of the operator's own cloud project. Any exposure of user data would depend on rules that the operator can confirm.

Fix: Restrict the key by package name and signing certificate, confirm deny-by-default rules for Firestore and Storage, and retire projects that the app no longer needs.

H4: Policy requires age 18, Play rating is PEGI 3, onboarding strings show no age step

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

The privacy policy states: ”You must not use YO unless you are aged 18 or older.” The live Google Play content rating is PEGI 3, read twice on the fetched listing page. The onboarding keys in en.json show two acceptance checkboxes, Terms of Service and Data Privacy Policy, then account creation and email verification. No date of birth field and no age verification step appears in the onboarding strings or the Dart path strings. The only age field, settings.user_data.age, is entered after account creation for the test report. The three signals do not agree. The statement that no age check exists is drawn from strings, because Dart compiled to ARM64 code was not disassembled, so it is recorded as an observation. It was disclosed as HIGH on 22 August 2026.

```
Privacy policy: You must not use YO unless you are aged 18 or older.
Google Play content rating: PEGI 3
Onboarding: Terms of Service checkbox, Data Privacy Policy checkbox, account creation,
     email verific
    ation
Age field: settings.user_data.age, after account creation
```

Impact: The question is whether a minor can create an account for a reproductive health device. The strings alone cannot answer it.

Fix: Answer question 3 of the notice: state what measure keeps minors out and whether an impact assessment exists.

M2: Marketing messages tied to account creation

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

The privacy policy states: ”Marketing consent: You will receive marketing and new content communications from us if you have created an account. You can ask us to stop sending you marketing messages by changing the communication preferences in your account with us.” Account creation is required to run a test. The wording ties marketing to the same act and offers opting out only afterwards, which raises the question of a separate choice at signup. The finding rests on policy text and does not carry a CVSS score. It was disclosed as MEDIUM on 22 August 2026.

```
Marketing consent: You will receive marketing and new content communications from us
    if you have cre
    ated an account.
```

Impact: A person who wants to run a test receives marketing communications unless they change a setting afterwards.

Fix: Offer marketing as a separate choice at signup.

M3: Two legal entities named as operator, no EU representative named

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

The Play Store developer section names Medical Electronic Systems, LLC, 6345 Balboa Blvd Ste 185, Encino, CA 91316, United States, with itay@mes-ltd.com and +1 310-670-9066. The linked privacy policy names Medical Electronic Systems Limited, 20 Alon Hatavor Street, Caesarea Industrial Park, Israel 3088900, with support@yospermtest.com, and a data protection officer, Taly Vider Cohen. Neither document states how the two entities relate, and no representative in the Union is named in either. The findings notes record that Israel has a Commission adequacy decision (2011/61/EU), so the difference of entities is not by itself a transfer finding. A representative under Article 27 is required of a controller outside the Union that falls under Article 3(2). That applicability was not established beyond the public availability of the listing. It was disclosed as MEDIUM on 22 August 2026.

```
Play Store: Medical Electronic Systems, LLC, 6345 Balboa Blvd Ste 185, Encino, CA
    91316, United Stat
    es, itay@mes-ltd.com, +1 310-670-9066
Privacy policy: Medical Electronic Systems Limited, 20 Alon Hatavor Street, Caesarea
    Industrial Park
    , Israel 3088900, support@yospermtest.com
DPO named in the policy: Taly Vider Cohen
```

Impact: A person who wants to send an access or deletion request cannot tell from the two documents which entity answers it.

Fix: State which entity is the controller, how it relates to the other, and name a representative in the Union if Article 3(2) applies.

Impact Analysis

Three groups of people stand in the path of these mechanisms.

The first group is the users of the device. They test a semen sample at home. The sample video is analysed in the cloud, the app's analytics component starts before the acceptance screens can appear, and the store label says no data is shared with third parties while the policy names Firebase, BigQuery, Co-pilot CX Ltd and affiliates.

The second group is the partners of users. The profile holds a field about whether the partner tracks ovulation. The partner has no notice and no consent screen.

The third group is anyone who can reach the app and is under 18. The policy excludes them, the store rating admits all ages, and the onboarding strings show no age step.

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 22 Aug 2026	C4
Firebase starts before the acceptance screens can render	Manifest, directBootAware, initOrder 100	C3
The person connects the phone to the device's own WiFi	Location dialog, network security config	C1
The sample video is played from a stream allowed in cleartext	libmpv.so, cleartext exception	C1
The video goes to a cloud analysis service, a development instance is named in the app	Dart paths, endpoints	C2
Login runs through an external provider, the partner's status sits on the profile	com.copilot classes, partner field	C4, H2
The operator's support system acknowledges the notice automatically	Tickets 27089, 27375, 27895, 28228	All

The weak link of the chain is the same in C1 and C2: the package shows what is permitted and what is referenced, and only the operator can say what actually travels and where.

Inference Data, Bystanders and Control

Six categories of invisible data were considered. Non-events do not apply, because the app has no continuous monitoring surface. A household graph is confirmed in H2. A relationship graph from notifications does not apply, because no notification listener service exists. Bystander data applies mainly through the partner field, since the sample itself belongs to the account holder. Inference data is confirmed: the cloud pipeline computes motility and concentration scores from raw video, and these derived scores are more sensitive than the video metadata. Control data was checked and is clean. The Remote Config references trace to Crashlytics' own rollout subsystem, and no app-level remote command surface was found.

Consumer Protection & Platform Disclosures

The Data Safety section is a statement by the developer about the developer's own app. It says no data is shared with third parties. The operator's own policy states the opposite in its own words, which is the core of C4.

The content rating is PEGI 3 for a Class II reproductive health diagnostic product whose policy requires age 18 (H4). The notice is addressed to the operator and not to the platform.

Data Protection: Article by Article

Article	Relevance	Finding
5(1)(a), 5(2)	Transparency and accountability: label against policy, project sprawl	C3, C4, M1
5(1)(b), 5(1)(c)	Purpose and minimisation: location scope, partner field	H1, H2
5(1)(f), 32(1)(a), (b)	Cleartext exception, development endpoint, pinning, exposed key	C1, C2, H3, M1
6(1), 7(1), 7(4)	Consent before processing, marketing bundled with account creation	C3, M2
8	Age of consent for an information society service offered directly to a child, where consent is the basis	H4
9	Semen analysis results, partner's tracking status	C1, H2
13(1)(a), (c), (e), 14	Controller identity, purposes, recipients, information to the partner	M3, H1, C4, H2
25, 30	Design, records of processing	C2, M1
27	Representative in the Union, if Article 3(2) applies	M3
28	Processor agreement with the authentication provider	C4
35	Impact assessment for location and age risk	H1, H4

Regulatory & Legal Landscape

The bases are Regulation (EU) 2016/679 (GDPR) with Articles 5, 6, 7, 8, 9, 13, 14, 25, 27, 28, 30, 32 and 35. 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 has two named entities, one in the United States and one in Israel, and no disclosed main establishment in the Union, so 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.

The report makes no comparison with other applications.

Indicators of Compromise & Reproducible Evidence

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

```
Package       com.mes.YO_3_0.official_yo_3_0 257.0.5.1 (576)
XAPK          c909b2e3ecbf4e2152389d4feefcb561ee5c48012c5debf34add7289daf71c2e
base.apk      d0d8e3a52fc2c0150f2fa8fc58d8c0f3cee689e4f20ec8426f6235156e974fcb
arm64 split   2d6da8d9bd36452984c209fda87e62b4ef1b18313c958d876e0f1a8db16e7f8d
Firebase      project yo-home-sperm-test, bucket yo-home-sperm-test.appspot.com,
    sender 377022562223
API key       AIzaSyCpYg8w4so7r5H2qL3QJ7ozHf8rTI3rbc4
App ID        1:377022562223:android:7fc0b787961d18f88fb95a
Provider      com.mes.YO_3_0.official_yo_3_0.firebaseinitprovider (initOrder 100,
    directBootAware)
Cleartext     http://192.168.0.1, rtsp://192.168.0.1
Endpoints     us-central1-yodatacenter.cloudfunctions.net, us-central1-yohome-2019.
    cloudfunctions.ne
    t
              yoanalysis-wucicmh3qa-uc.a.run.app, yo-dev-analysis-wucicmh3qa-uc.a.run.
    app
Co-pilot      sphere.bycopilot.com/v2/partner/{partnerId}/acquire_ticket
Libraries     lib/arm64-v8a/libmpv.so (12.4 MB), libmediakitandroidhelper.so
Policy        https://yospermtest.com/yo3-data-privacy-policy/
Contacts      support@yospermtest.com, itay@mes-ltd.com, tickets 27089, 27375, 27895,
    28228
```

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

Disclosure Timeline & Outcome

Date	Event
22 Aug 2026	Notice REF YOHOMESPERMTEST-2026-R1 at 17:10 UTC to support@yospermtest.com and itay@mes-ltd.com, Datenschutzbehörde and EDPS in copy. Eleven findings, three questions, publication stated as 20 November 2026. Automatic acknowledgement at 17:11 UTC, ticket 27089.
12 Sep 2026	16:31 UTC follow-up: no reply of any kind after 21 days, open points restated. Automatic acknowledgement at 16:32 UTC, ticket 27375.
17 Oct 2026	18:55 UTC follow-up 34 days before publication, 56 days after the notice, from security@rfi-irfos.com. Automatic acknowledgement on 18 Oct 2026 at 19:22 UTC, ticket 27895.
15 Nov 2026	12:58 UTC message from s.kepp@rfi-irfos.com, 5 days before publication, 85 days after the notice, repeating the three questions. Automatic acknowledgement at 12:59 UTC, ticket 28228.
20 and 21 Nov 2026	Embargo date 20 November 2026, unchanged since 22 August 2026, passed without a substantive reply. No message from the operator beyond the four automatic acknowledgements. Final report published on 21 November 2026.

Outcome as of 21 November 2026: four automatic acknowledgements, no substantive reply, no answer to any of the three questions.

What the Operator Got Right

allowBackup is false, which blocks adb backup of local app data. The cleartext exception is narrow, one local address and not a blanket allowance, and the application default is usesCleartextTraffic false. Firebase App Check with Play Integrity appears integrated on the client side (getInstalledAppCheckProviderFactory, generatePlayIntegrityChallenge, exchangePlayIntegrityToken), although server-side enforcement was not verified. Biometric Smart Login is opt-in and explained to the user. The privacy policy has a working data subject rights section with a one month response commitment, and names a data protection officer. The retention statement for results data gives an explicit ceiling of about one year. The calendar permissions serve a single next-test reminder through the add_2_calendar plugin and are not a hidden capability. The app requests no camera, microphone, Bluetooth or contacts permission.

Residual Risk & Recommendations

Priority	Action	Finding
1	State which of label and policy is correct, confirm the processor agreement with the authentication provider and correct the Data Safety label	C4
2	State what protects the sample video on the local link and on the way to the cloud	C1, C2
3	Remove the development endpoint from production builds	C2
4	Start Firebase measurement after the acceptance step	C3
5	State where the partner field is stored and how the partner is informed	H2
6	Drop background location or explain it, and align the policy with the dialog	H1
7	Describe the age check and align the policy, the rating and the onboarding	H4
8	Restrict the Google key, confirm rules, add pinning, retire unused projects	M1, H3
9	Name the controller and a representative in the Union if Article 3(2) applies, offer marketing as a separate choice	M3, M2

Residual risk: the Dart code that holds the upload, the age handling and the partner field was not disassembled, and no traffic was captured. This report describes version 257.0.5.1 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 listing and privacy policy. No endpoint was called, the key was not tested and no traffic was captured. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Arts. 5, 6, 7, 8, 9, 13, 14, 25, 27, 28, 30, 32, 35. RFI-IRFOS ZVR 1015608684, GISA 39261441. REF YOHOMESPERMTEST-2026-R1.