Security & Privacy Disclosure, Final Report

ExSeed, home sperm test companion app for Android (com.exseedhealth.app)

A fertility test app whose Play label declares no health data, a pre-consent tracking start and an EU contact in London.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. EMBARGO 20 NOVEMBER 2026. ONLY AUTOMATED AI-AGENT REPLIES, NO SUBSTANTIVE REPLY.

Target	ExSeed Health Ltd, London, United Kingdom (Company No. 11002717)
Versions Audited	1.10.4 / versionCode 252, analysed 2026-08-22
Notice / Publication	2026-08-22 / 2026-11-20 (90 days)
Findings	9: 2 Critical, 2 High, 4 Medium, 1 observation
Status	ONLY AUTOMATED AI-AGENT REPLIES (22 AUGUST, 18 OCTOBER, 15 NOVEMBER 2026), NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`90102f1c790423027201c2721da81effbf2fa178c0c2bef3ac89830d7e7aaa84`

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 5

6 Findings 6

6.1 C1: The Google Play Data Safety label lists no health data, no photos or videos and no personal info for an app that records a biological sample on video . . . 6

6.2 C2: Firebase and Google Measurement start with the app process, before any consent screen, with no consent platform in the binary, on a paid medical product 7

6.3 C3: A Firebase project key and a Google Maps key are hardcoded in the distributed binary, next to the project's database URL 8

6.4 H1: No age assurance beyond a self-declared 18+ acknowledgement, against a PEGI 3 rating 9

6.5 H2: The privacy policy names a UK data protection officer and no Article 27 representative in the EU 10

6.6 H3: RECORD_AUDIO and a custom MediaRecorder pipeline sit beside the sample video, with no stated purpose for sound 11

6.7 H4: A generic multi-jurisdiction privacy template never names the fertility results, the sample video or the impact assessment 12

6.8 M1: No certificate pinning, system trust anchors only 13

6.9 M2: Firebase Remote Config is registered, the package cannot show whether it is used 13

7 Impact Analysis 14

8 The Complete Chain 14

9 Reproductive Health Data and Bystanders 15

10 Data Protection: Article by Article 15

11 Platform Disclosures: Google Play Data Safety 16

12 Regulatory & Legal Landscape 16

13 Indicators of Compromise & Reproducible Evidence 17

14 Disclosure Timeline & Outcome 18

15 What ExSeed Got Right 18

16 Residual Risk & Recommendations 19

Executive Summary

ExSeed is the companion app for a CE-marked home sperm test. Users clip a lens to the phone, record a sample on video and receive concentration, motility and volume results that they can pass to a doctor. It is published on Google Play by ExSeed Health Ltd of London under the package com.exseedhealth.app, with 50,000 or more downloads, a Medical device badge and a PEGI 3 rating. On 22 August 2026 RFI-IRFOS disclosed nine findings from a root level code analysis of version 1.10.4 under REF EXSEED-2026-R1.

The package contains no on-device analysis model, so the sample video leaves the phone for api.exseedhealth.com. The people who use the app have bought a diagnostic device to test something private and often worrying. The sharpest gap lies between what the product is and what its own Google Play Data Safety label says. The label lists location and crash logs. It lists no health data, no photos or videos and no personal info (C1).

Three more findings carry the weight. Firebase and Google Measurement start with the process, before any consent screen, and the binary holds no consent platform (C2). A Firebase key and a Maps key are hardcoded in every copy, next to the project's database URL (C3). The privacy policy names a UK data protection officer and no Article 27 representative in the Union (H2). The remaining findings are the age gate (H1), the audio permission beside the sample video (H3), the generic privacy notice (H4), the missing pinning (M1) and the Remote Config observation (M2).

The notice of 22 August 2026 went to the data protection officer and the support address with the Austrian DSB, the EDPS and the UK ICO in copy. Within two minutes the support desk's AI agent answered and pointed to the data protection officer. A follow-up on 17 October 2026 repeated three questions, and the support desk answered again on 18 October 2026 with the postal address of the officer. A further follow-up on 15 November 2026, five days before the embargo date, drew a third reply from the same AI agent with the same pointer. No person has answered a finding or a question. This report is published after the embargo date of 20 November 2026 was reached.

Scope: Root level code analysis of the Google Play release 1.10.4 (versionCode 252): manifest, resources, network security config and the dex string pool of seven classes*.dex files. The Google Play Data Safety page and the privacy policy at www.exseedhealth.com/privacy-policy/ were read from the public sites on 22 August 2026. No ExSeed server, database or API key was called, no account was created, no sample was recorded, no traffic was captured and no runtime instrumentation was used. Items the package cannot show are marked UNVERIFIED.

ID	Severity	Title
C1	CRITICAL	The Google Play Data Safety label lists no health data, no photos or videos and no personal info for an app that records a biological sample on video
C2	CRITICAL	Firebase and Google Measurement start with the app process, before any consent screen, with no consent platform in the binary, on a paid medical product
C3	HIGH	A Firebase project key and a Google Maps key are hardcoded in the distributed binary, next to the project's database URL
H1	MEDIUM	No age assurance beyond a self-declared 18+ acknowledgement, against a PEGI 3 rating
H2	HIGH	The privacy policy names a UK data protection officer and no Article 27 representative in the EU
H3	MEDIUM	RECORD_AUDIO and a custom MediaRecorder pipeline sit beside the sample video, with no stated purpose for sound
H4	MEDIUM	A generic multi-jurisdiction privacy template never names the fertility results, the sample video or the impact assessment
M1	MEDIUM	No certificate pinning, system trust anchors only
M2	INFO	Firebase Remote Config is registered, the package cannot show whether it is used

Finding Status at a Glance

ID	Disclosed	This report	Status on 21 November 2026
C1	CRITICAL	CRITICAL	Open. Question 1 unanswered.
C2	CRITICAL	CRITICAL	Open. Question 2 unanswered.
C3	CRITICAL	HIGH	Open. Version 1.10.4 analysed on 22 August 2026.
H1	HIGH	MEDIUM	Open. No answer received.
H2	HIGH	HIGH	Open. Question 3 unanswered.
H3	HIGH	MEDIUM	Open. Capability shown, upload not shown.
H4	HIGH	MEDIUM	Open. Question 3 unanswered.
M1	MEDIUM	MEDIUM	Open. No answer received.
M2	MEDIUM	INFO	Observation. Use of Remote Config not shown.

Subject & Operator Analysis

The privacy policy names ExSeed Health Ltd (ExSeed Health Limited), Company No. 11002717, as controller, with its office at Office 8, 6 Hooker's Road, c/o Yonder Office, London, E17 6DP, United Kingdom. The policy names a data protection officer, Emil Andersen, ea@exseedhealth.com, and a support address, support@exseedhealth.com. No press contact was found. No Article 27 representative is named.

The product is the ExSeed Device, marketed as a CE-marked in-vitro diagnostic home sperm test. The Play listing shows Health & Fitness as category, a Medical device badge, 50,000 or more downloads and a PEGI 3 rating. The listing was served under the Austrian storefront on 22 August 2026. The operator is established in the United Kingdom, which makes it a third-country controller under the GDPR. The UK Information Commissioner is the regulator of its home state and the Austrian Datenschutzbehörde is the authority for a matter that starts in Austria.

Architecture & Data Flow

The app is a native Android application with seven dex files and a base APK of 106.1 MB (139.1 MB with the arm64 and mdpi splits). The camera pipeline is the operator's own code with camera2-* tags built on MediaRecorder, not a camera library. The only machine learning models in the package are Google ML Kit barcode models used to pair the device by QR code. No model that analyses sperm video was found, so the analysis runs on the server side and the video is sent to api.exseedhealth.com. Two AWS API Gateway endpoints found in the strings resolve to AWS eu-central-1 in Frankfurt. The user account runs on AWS Cognito. Google Firebase supplies Analytics, Messaging, Performance and Remote Config. Intercom provides customer support chat. Firebase starts through a ContentProvider before any screen. Cleartext traffic is denied for the whole app and the app trusts system certificates only.

Engagement Summary

The notice REF EXSEED-2026-R1 was sent on 22 August 2026 at 17:05 UTC to ea@exseedhealth.com and support@exseedhealth.com, with dsb@dsb.gv.at, edps@edps.europa.eu and icocasework@ico.org.uk in copy. It listed the critical findings with verbatim evidence, summarised four high and two medium findings, credited what ExSeed does well and asked three questions.

Two minutes later, at 17:07 UTC, the support desk replied through Fin, ExSeed Health's AI agent. The reply calls the notice a technical and regulatory report, names the data protection officer as the right contact, and recalls that the privacy notice speaks of consent and of ISO 27001. It addresses no finding.

A follow-up from security@rfi-irfos.com went to the same two addresses on 17 October 2026 at 19:34 UTC, 34 days before the embargo date. It listed C1, C2, C3 and H2 as open and repeated the three questions. On 18 October 2026 at 19:09 UTC the support desk answered again, repeated the postal address of the data protection officer and called it the designated channel. That message addresses no finding and no question either.

On 15 November 2026 at 12:58 UTC a further follow-up went from s.kepp@rfi-irfos.com, five days before the embargo date. At 13:00 UTC the AI agent answered a third time with the

same pointer to the data protection officer and added that the customer care team can also be reached at support@exseedhealth.com. All three replies copied the supervisory authorities from the first notice. No message from the data protection officer or from any other person at ExSeed is on record.

Findings

C1: The Google Play Data Safety label lists no health data, no photos or videos and no personal info for an app that records a biological sample on video

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), disclosed as CRITICAL on 22 August 2026, open, rated CRITICAL by blast-radius escalation

The label fetched on 22 August 2026 declares Location and Crash logs as the only collected data and Location, Crash logs, Other in-app messages and App interactions as shared. It has no entry for Health and fitness, Photos and videos or Personal info. The app records a sperm sample on video, requires an AWS Cognito account with email and password and exports a medical report for the user's doctor. No on-device analysis model is in the package, only Google ML Kit barcode models for device pairing, so the sample video leaves the phone for api.exseedhealth.com. This is a transparency finding with no technical attack path, so the CVSS vector carries no impact. RFI-IRFOS blast-radius escalation: raised from none to CRITICAL because the label is the one document a prospective user reads before installing, the product is a CE-marked diagnostic that handles reproductive health data, and the omission covers three entire data categories. The score is zero because no technical vector exists.

```
Data shared:
  Location (Approximate + Precise)  - Analytics
  Crash logs, Diagnostics           - Analytics
  Messages: "Other in-app messages" - App functionality
  App interactions                  - Analytics

Data collected:
  Location (Approximate + Precise)  - Optional - App functionality, Analytics

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

Not present: Health and fitness, Photos and videos, Personal info
```

The Play listing describes the function itself: home testing of volume, motility and concentration through the phone, with results exported to a doctor or clinic. The manifest requests android.permission.CAMERA. The package ships the AWS Cognito sign-up, login and MFA activities (com.amazonaws.mobile.auth.userpools). The label and the product disagree on three whole categories.

Impact: A man or a couple deciding whether to install a fertility test read the Data Safety label to learn what the app takes. The label tells them it takes an approximate location and crash logs. It does not tell them that a video of the sample, their email address and their fertility

results are stored by the operator. The people misled are people at a moment of worry about their own reproductive health.

Fix: Complete the label for Health and fitness, Photos and videos and Personal info, and state the retention of the sample video. Publish the corrected label before the next release.

C2: Firebase and Google Measurement start with the app process, before any consent screen, with no consent platform in the binary, on a paid medical product

---

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, open, rated CRITICAL by blast-radius escalation

FirebaseInitProvider is declared directBootAware with initOrder 100, so Firebase registers before any Activity can draw a consent screen. AppMeasurementReceiver and AppMeasurementService are enabled with no gating flag in the manifest. A search across all seven classes*.dex files, about 807,000 extracted strings, for OneTrust, Didomi, Usercentrics, consentmanager and cmp_sdk returned zero hits. The IAB TCF strings present (IABTCF_CmpSdkID, IABTCF_TCString) are inert library constants. The 2,940 entries of res/values/strings.xml hold no consent or cookie choice text. Scope: this finding covers general app telemetry. What the telemetry contains was not measured and no traffic was captured. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to CRITICAL because the product is a paid diagnostic for reproductive health, initialisation can occur before the device is unlocked and no consent mechanism of any kind exists in the binary. The CVSS vector scores only the technical exposure of low-sensitivity telemetry.

```
<provider android:authorities="com.exseedhealth.app.firebaseinitprovider"
          android:directBootAware="true" android:exported="false"
          android:initOrder="100"
          android:name="com.google.firebase.provider.FirebaseInitProvider"/>

<receiver android:enabled="true" android:exported="false"
          android:name="com.google.android.gms.measurement.AppMeasurementReceiver"/>
<service android:enabled="true" android:exported="false"
         android:name="com.google.android.gms.measurement.AppMeasurementService"/>

grep -i "onetrust|didomi|usercentrics|consentmanager|cmp_sdk"  (7 dex files)  ->  0
    hits
```

The people who install this app have already bought a CE-marked diagnostic device. The argument that tracking pays for a free app does not apply to them. Initialisation is identical for every user and happens before the device is paired.

Impact: A person who has just bought a fertility test and opens the app for the first time has no choice to make about telemetry, because it starts with the process. The device that runs a test for male fertility starts sending usage signals to Google before the user has seen a single screen.

Fix: Disable automatic collection in the manifest and initialise Firebase Analytics and Crashlytics only after a recorded consent decision. Add a consent screen that records the choice per purpose.

C3: A Firebase project key and a Google Maps key are hardcoded in the distributed binary, next to the project's database URL

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 CRITICAL on 22 August 2026, open, rated HIGH by blast-radius escalation

Two Google API keys sit in clear text in every distributed copy of the app. The Firebase project key belongs to the project exseed-health and the Maps Platform key serves the clinic finder. Google documents such keys as non-secret by design, so this is an availability finding and not a confidentiality finding. A quota or billing exhaustion against either key can take Firebase services registered on the project, or the clinic finder, offline. The extracted database URL means that a Realtime Database may exist for the project. Whether its Security Rules and the key restrictions in Google Cloud Console are correct is not shown by the package. No call was made against either key or against the database. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.3 to HIGH because the project backs an account system for fertility test results and the key cannot be rotated for installed copies. The CVSS vector scores only the availability exposure that the package demonstrates. This label is lower than the CRITICAL of the notice of 22 August 2026 because no call was made against the project and the Security Rules are not shown by the package.

```
<!-- res/values/strings.xml -->
<string name="google_api_key">AIzaSyAwELRBWAkou0MNizXEU2V84l8p0BUOOJA</string>
<string name="google_app_id">1:400871371771:android:453b07aeeb050e48</string>
<string name="project_id">exseed-health</string>
<string name="firebase_database_url">https://exseed-health.firebaseio.com</string>
<string name="gcm_defaultSenderId">400871371771</string>
<string name="default_web_client_id">400871371771-vr44kl7t4ikc9buqjf6vf36uo7f7t9q7.
    apps.googleusercontent.com</string>

<!-- AndroidManifest.xml -->
<meta-data android:name="com.google.android.geo.API_KEY"
           android:value="AIzaSyCqKtgbA7w81YN2qj8r9WL05UH3lM0bNH8"/>
```

The notice of 22 August 2026 named five abuse paths that follow from the extracted values: quota and billing exhaustion, project enumeration, unauthenticated Realtime Database read, unauthenticated write, and Remote Config reconnaissance. Paths three and four depend on Security Rules that this report does not claim to know.

Impact: The key cannot be rotated for installed copies without an app update. If the project is rate-limited or billed out, sign-in, push messages and the clinic finder stop for people who are waiting on a fertility result or looking for a clinic. If the database rules are loose, records of a very private test sit behind a URL printed in the app.

Fix: Restrict both keys by package name, signing certificate and API scope. Enforce App Check for the Realtime Database. Send the Security Rules and the quota settings as evidence.

H1: No age assurance beyond a self-declared 18+ acknowledgement, against a PEGI 3 rating

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), disclosed as HIGH on 22 August 2026, open, rated MEDIUM by blast-radius escalation

The EULA text in res/values/strings.xml has the user confirm that they are 18 years of age or older. No date-of-birth field and no age verification vendor integration (Persona, Yoti, Veriff or similar) was found in the 807,000-string corpus. The Play listing fetched on 22 August 2026 shows PEGI 3. The product tests male fertility and exports reproductive health results, so the audience is adult by the operator's own text. A checkbox stops no one. The rating is not a GDPR finding. The missing age assurance on a reproductive health product is a transparency and design matter, so the CVSS vector carries no impact. RFI-IRFOS blast-radius escalation: raised from none to MEDIUM because the data is reproductive health data and the only age control is a self-declaration. The score is zero because no technical vector exists.

```
res/values/strings.xml:166  "By using the application, you (A) acknowledge that you
    have read and
  understand this agreement, (B) confirm that you are 18 years of age or older /
  of legal age to enter into a binding agreement..."
res/values/strings.xml:238  "...you attest that you are 18 years of age or older / of
    legal age to enter
  into a binding agreement..."

Play Store content rating (fetched 2026-08-22): PEGI 3
```

The notice of 22 August 2026 rated this finding HIGH. This report rates it MEDIUM, because the text itself shows the audience is adult and the rating question belongs to the platform rather than to the processing.

Impact: A teenager who finds a rating of "suitable for all ages" and a one-tap acknowledgement can set up an account, record a sample and receive reproductive health results with nobody to ask whether he is old enough to understand them.

Fix: State the real audience in the store listing and add an age screen that does more than a checkbox, proportionate to the data, or document why none is needed.

H2: The privacy policy names a UK data protection officer and no Article 27 representative in the EU

HIGH, 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), disclosed as HIGH on 22 August 2026, open, rated HIGH by blast-radius escalation

The controller is ExSeed Health Ltd, Company No. 11002717, registered at 6 Hooker's Road, London E17 6DP. After the UK left the EU the controller is a third-country entity under the GDPR. The privacy policy fetched on 22 August 2026 names a DPO, Emil Andersen, ea@exseedhealth.com. It does not name an Article 27 representative in any section, including the contact section. The Play listing was served under the Austrian storefront. The core function processes reproductive health results, which are special-category data under Article 9, so the exemption in Article 27(2) is unlikely to cover the processing. The operator's total EU user volume is not known from the package. This is a legal and transparency finding with no technical attack path, so the CVSS vector carries no impact. RFI-IRFOS blast-radius escalation: raised from none to HIGH because the data concerns reproductive health, the rights holders are users who have no other local contact, and the role cannot be exercised through a London address. The score is zero because no technical vector exists.

Controller: ExSeed Health Ltd (ExSeed Health Limited), Company No. 11002717, Office 8, 6 Hooker's Road, c/o Yonder Office, London, E17 6DP, United Kingdom. Data protection contact named in the policy: Emil Andersen, ea@exseedhealth.com. Article 27 representative named in the policy: none.

Impact: A person in Austria or Germany who wants a copy or deletion of a fertility video and the results from it has a London address and an email address as the only contact. Supervisory authorities in the Union have no Member State address to write to.

Fix: Designate a representative established in a Member State where users live and publish the name and address in the policy the app links to.

H3: RECORD_AUDIO and a custom MediaRecorder pipeline sit beside the sample video, with no stated purpose for sound

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.8 (CVSS-B), disclosed as HIGH on 22 August 2026, open

The manifest requests android.permission.RECORD_AUDIO and declares android.hardware.microphone as not required. The dex files hold the operator's own capture code with camera2-* log tags (camera2-setupMediaRecorder, camera2-onFinishRecordingInfo) next to android.media.MediaRecorder and android.media.AudioRecord. Sperm concentration and motility analysis from video needs no sound. The package shows no code that mutes or strips the audio track and no sign that it is kept. Whether the audio is recorded, kept in the uploaded file or discarded on the phone is UNVERIFIED, because that needs observation of the running capture and upload path, which this analysis does not do.

```
<uses-permission android:name="android.permission.RECORD_AUDIO"/>
<uses-feature android:name="android.hardware.microphone" android:required="false"/>

camera2-setupMediaRecorder
camera2-onFinishRecordingInfo
camera2-onImageAvailableListener
Landroid/media/MediaRecorder;
Landroid/media/AudioRecord;
```

The notice of 22 August 2026 rated this finding HIGH. This report rates it MEDIUM, because the package shows the capability and not the transmission of sound.

Impact: If sound travels with the video, a partner's voice, a child in the next room or a conversation in a private room is recorded during a very private moment. Those people are not the account holder and have agreed to nothing.

Fix: State in the policy whether sound is recorded. Disable the audio track in the recorder configuration if no function needs it, and request the permission only if one does.

H4: A generic multi-jurisdiction privacy template never names the fertility results, the sample video or the impact assessment

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), disclosed as HIGH on 22 August 2026, open, rated MEDIUM by blast-radius escalation

The privacy notice covers EEA and UK GDPR, Canada, California and Virginia in broad template language. It speaks of sensitive personal information "when necessary" and links to a section on sensitive information. It does not name the data types the product creates and stores: sperm concentration, motility and volume results and the sample video. No Article 35 impact assessment is referenced, although the operator markets an IVD CE-certified home diagnostic and ISO 27001 alignment. An assessment may exist and may simply not be mentioned in the public notice. The notice of 22 August 2026 asked for it as a question. This is a legal and transparency finding with no technical attack path, so the CVSS vector carries no impact. RFI-IRFOS blast-radius escalation: raised from none to MEDIUM because the notice is the user's only written explanation of how reproductive health results are handled and it does not name them. The score is zero because no technical vector exists.

Source: www.exseedhealth.com/privacy-policy/, read on 22 August 2026. The page text is not archived in the case folder, so the quotation above is a paraphrase of the read text and the page should be re-read before publication.

Impact: A user who wants to know what happens to the video of a sample, the results and the report sent to a doctor finds a notice written for every kind of app. The health data the user has just created is not named once.

Fix: Name the fertility results, the sample video and any audio as health data in the notice. State the legal basis, the retention, the recipients and the outcome of the impact assessment.

M1: No certificate pinning, system trust anchors only

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 MEDIUM on 22 August 2026, open

res/xml/network_security_config.xml sets cleartextTrafficPermitted to false for the whole app, which is correct and credited below. It trusts the system certificate store and declares no pin-set for api.exseedhealth.com or any other host. A device with a hostile or enterprise-installed root certificate can let a third party sit in the TLS connection that carries the fertility results. The attacker position required is strong.

```
<network-security-config>
    <base-config cleartextTrafficPermitted="false">
        <trust-anchors>
            <certificates src="system" />
        </trust-anchors>
    </base-config>
</network-security-config>
```

Impact: Anyone who can place a certificate on a phone, for example a managed work phone or a compromised device, could read the traffic that carries a person's fertility results.

Fix: Add a pin-set for api.exseedhealth.com and for the other backends the operator controls, with a backup pin.

M2: Firebase Remote Config is registered, the package cannot show whether it is used

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

Firebase Remote Config is registered in the ComponentDiscoveryService through RemoteConfigRegistrar. The operator's backend therefore has the technical ability to change feature flags after installation without a new release. Which flags exist, and whether any of them touches camera or microphone behaviour or upload triggers, is UNVERIFIED and cannot be read from the package. The GDPR is not engaged by the registration itself. The finding is recorded as a standing architectural fact and carries no score.

```
<meta-data android:name="com.google.firebase.components:com.google.firebase.
    remoteconfig.RemoteConfigRegistrar"
           android:value="com.google.firebase.components.ComponentRegistrar"/>
```

The notice of 22 August 2026 rated this finding MEDIUM. This report records it as an observation, because a registered library is not a defect.

Impact: The operator can change what the app does after installation without a new release. That is normal practice, and it matters for the sensors only if a flag ever reaches them.

Fix: State in the policy which behaviours Remote Config controls and confirm that no flag changes sensor or upload behaviour.

Impact Analysis

The people affected are men and couples who test fertility at home. The test is paid for, and the buyers act at a moment of concern about reproductive health. Many open the app for the first time after the device has arrived, with a sample ready to record. They read the Play label before installing and trust it to say what the app takes. The label tells them very little (C1).

The sample video, the account and the results are the most private material the app handles. A partner or a child who is in the room while a sample is recorded is a bystander to that moment, and the audio permission puts them in range of the microphone (H3). Users in the Union who want to exercise access or deletion rights find only a London address (H2).

The app is used by one person at a time on a personal phone. No finding in this report affects people who do not use the app, except for bystanders in H3.

The Complete Chain

Step 1, store: a person finds the app on Google Play, sees PEGI 3, a Medical device badge and a Data Safety label that lists location and crash logs (C1, H1).

Step 2, install and first launch: FirebaseInitProvider starts with the process, before any screen and before pairing. Analytics and Measurement run without a consent decision (C2).

Step 3, account: the user creates a Cognito account with email and password and confirms in one acknowledgement that he is 18 or older (H1).

Step 4, sample: the user records a sample on video through the operator’s own capture pipeline, which holds an audio recorder (H3). The video goes to api.exseedhealth.com. No model in the package analyses it on the phone.

Step 5, results: the results are shown, stored and exported as a medical report. The notice that describes this handling is a generic template that does not name the data (H4).

Step 6, rights: the user wants a copy or deletion and finds a UK officer and no representative in the Union (H2). The Firebase and Maps keys in the package belong to the project that carries sign-in, push messages and the clinic finder (C3). The connection to the backend trusts any certificate in the device store (M1).

Reproductive Health Data and Bystanders

Fertility test results are health data under Article 9 GDPR. They also say something about a person's sexual and reproductive life, and for many couples they sit in the middle of a private decision. The app handles three kinds of material that belong to this group: the sample video, the numerical results and the exported medical report.

Bystander data is a separate point. A voice recorded while a partner is in the room, or a child in the next room, belongs to a person who made no decision about the app. Whether the audio track is recorded and kept is UNVERIFIED (H3). If it is not, the permission and the recorder configuration are still a design choice that the operator can close in one release.

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1, H1 and H4.

Article 5(1)(b) and (c), purpose limitation and data minimisation: engaged by H3. Sound has no function in a video analysis of a sample.

Article 5(2), accountability: engaged by C1, C2 and C3. The controller carries the burden of showing a correct label, consent gating and correct key and database restrictions.

Article 6(1)(a) and Article 7(1), lawful basis and conditions for consent: engaged by C2. Telemetry that starts before a consent decision has no consent to rest on.

Article 8, child's consent: context for H1. Not engaged for adult users.

Article 9, special categories: engaged by H3 and H4. The notice never names the health data it covers.

Article 12(1) and Article 13(1)(a), (c) to (e): engaged by C1, H2 and H4.

Article 25, data protection by design and by default: engaged by C2 and C3.

Article 27(1) and (2), representative: engaged by H2.

Article 32(1)(a) and (b), security of processing: engaged by C3 and M1.

Article 35, impact assessment: asked as a question in H4. Large-scale processing of health data is a case the article is written for.

ePrivacy Directive Art. 5(3): engaged by C2, because storing or reading information on terminal equipment requires consent unless strictly necessary.

Platform Disclosures: Google Play Data Safety

The Data Safety label is a declaration made by the developer in Google Play Console. Google publishes it and asks developers to keep it accurate. This report attributes the content of the label to ExSeed Health Ltd and makes no claim about the conduct of the platform operator.

The label read on 22 August 2026 lists Location and Crash logs as the only collected data, and Location, Crash logs, Other in-app messages and App interactions as shared. It states that data is encrypted in transit and that deletion can be requested. The deletion statement matches the account deletion section of the privacy policy and is credited below. The label does not list Health and fitness, Photos and videos or Personal info. The page was not archived at the time of reading. It should be fetched again before publication.

The Play content rating of PEGI 3 is a store rating of the listing and is not a GDPR classification. It is cited in H1 as context.

Regulatory & Legal Landscape

The framework applied is the GDPR, with Article 27 for a controller outside the Union and Article 9 for health data, together with Article 5(3) of the ePrivacy Directive for terminal equipment. The operator is established in the United Kingdom and offers its product to users in the Union, which brings Article 3(2) GDPR into play. The UK GDPR applies to the operator in its home state, and the UK Information Commissioner is in copy of the notice for that reason.

The operator describes the device as CE-marked under the in-vitro diagnostic rules. This report does not assess the conformity of the device and takes the statement as the operator's own claim. No obligation under other digital regulation is asserted for this operator, because its classification has not been established.

The competent authority for an Austrian initiated matter is the Österreichische Datenschutzbehörde (dsb@dsb.gv.at). The European Data Protection Supervisor (edps@edps.europa.eu) is in copy under the standing practice of the programme. The disclosure follows ISO/IEC 29147 and Art. 17 StGG.

Indicators of Compromise & Reproducible Evidence

No indicators of compromise were found and none are claimed. The values below are the identifiers needed to reproduce each finding from the published package. All values are given in full.

```
Package            com.exseedhealth.app
Version            1.10.4 (versionCode 252), analysed 2026-08-22
minSdk / target    24 / 36
base APK SHA-256   90102f1c790423027201c2721da81effbf2fa178c0c2bef3ac89830d7e7aaa84
XAPK SHA-256       0681e8ea9b06ff4bd4e8f492a34fd2a01bb411dd08494918a1378c0a392e533a
Firebase project   exseed-health
Firebase API key   AIzaSyAwELRBWAkou0MNizXEU2V84l8p0BUOOJA
Google app ID      1:400871371771:android:453b07aeeb050e48
Sender ID          400871371771
Database URL       https://exseed-health.firebaseio.com
Web client ID      400871371771-vr44kl7t4ikc9buqjf6vf36uo7f7t9q7.apps.
    googleusercontent.com
Maps API key       AIzaSyCqKtgbA7w81YN2qj8r9WL05UH3lM0bNH8
Operator           ExSeed Health Ltd, Company No. 11002717
```

```
C1  https://play.google.com/store/apps/datasafety?id=com.exseedhealth.app (read
    2026-08-22)
C2  AndroidManifest.xml: FirebaseInitProvider (directBootAware=true, initOrder=100),
    AppMeasurement*
C2  CMP search over classes*.dex (7 files, about 807,000 strings): 0 hits
C3  res/values/strings.xml: google_api_key, firebase_database_url. AndroidManifest.xml
    : geo.API_KEY
H1  res/values/strings.xml lines 166 and 238. Play listing: PEGI 3
H2  www.exseedhealth.com/privacy-policy/ (read 2026-08-22)
H3  AndroidManifest.xml: RECORD_AUDIO. classes*.dex: camera2-setupMediaRecorder,
    MediaRecorder, AudioRecord
H4  www.exseedhealth.com/privacy-policy/ (read 2026-08-22)
M1  res/xml/network_security_config.xml
M2  AndroidManifest.xml: RemoteConfigRegistrar
```

Reproduction: obtain com.exseedhealth.app 1.10.4 from Google Play, check the SHA-256 above, decode the manifest and resources with apktool and read the named files. No device, account or network access is needed for the package findings.

Disclosure Timeline & Outcome

2026-08-22 Notice REF EXSEED-2026-R1 to ea@exseedhealth.com and support@exseedhealth.com, CC DSB, EDPS and UK ICO. Findings C1 to C3, H1 to H4 and M1, M2 with verbatim evidence, three questions asked.

2026-08-22 Two minutes later, reply from the support desk through Fin, ExSeed Health's AI agent, naming the data protection officer as the contact. No finding addressed.

2026-10-17 Follow-up from security@rfi-irfos.com to the same addresses, 34 days before the embargo date, with C1, C2, C3 and H2 as open and the same three questions.

2026-10-18 Reply from the support desk repeating the postal address of the data protection officer. No finding or question addressed.

2026-11-15 Follow-up from s.kepp@rfi-irfos.com at 12:58 UTC to the same addresses, five days before the embargo date.

2026-11-15 Third reply from Fin at 13:00 UTC, quoting thanks "for outlining the timeline and questions clearly", with the same pointer to the data protection officer and the customer care address. No finding or question addressed.

2026-11-20 Embargo date, 90 days after delivery of the notice of 22 August 2026.

2026-11-21 No reply from a person, no written position and no delivery failure notice on record.

What ExSeed Got Right

Cleartext traffic is denied for the whole app, with no domain exception. A named data protection officer is published with a postal address and the Companies House number. No SDK from sanctioned or high-risk jurisdictions was found in the 57 MB dex corpus, and the stack contains no advertising network, attribution SDK or session replay tool. The only third-party SDKs besides Google and AWS are Intercom for support chat. The two backend endpoints found in the strings resolve to AWS eu-central-1 in Frankfurt. The setting android:allowBackup is false. A real deletion mechanism exists, both on the Play label and in the privacy policy. The AWS region table in the strings includes Chinese region names, which is the standard table of the AWS SDK and is not treated as evidence of any use.

Residual Risk & Recommendations

Open at the date of publication: all nine items, with no written position from the operator as of 21 November 2026. Items that only the operator can close are the label in C1, the consent gate in C2, the key restrictions and database rules in C3, the age assurance in H1, the representative in H2, the audio configuration in H3, the privacy notice and impact assessment in H4 and the pin-set in M1.

Recommendations: correct the Data Safety label, gate Firebase Analytics and Crashlytics behind a recorded consent decision, restrict both Google keys by package, certificate and API scope and enforce App Check for the database, appoint a representative established in a Member State, remove the audio track from the sample recorder unless a function needs it, rewrite the privacy notice to name the fertility results and the sample video, publish the outcome of the Article 35 assessment, and add a pin-set for operator-controlled hosts.

Statements are limited to the package and the public documents named above.

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.

No ExSeed servers or accounts were probed. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. REF EXSEED-2026-R1.