Security & Privacy Disclosure, Final Report

Nix Solo for Android (com.nixbiosensors)

A hydration app that asks for your race, and starts its analytics before you can answer.

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

Target	Nix, Inc., 354 Winter Street, Norwell, MA 02061, USA (developer name on Google Play: Nix Biosensors)
Versions Audited	3.44.3 (versionCode 3044003), analysed 2026-08-22. Google Play showed an update on 2026-11-10, not analysed.
Supervisory Authority	None designated (operator outside the EU). Austrian Daten-schutzbehörde copied.
Notice / Publication	2026-08-22 / 2026-11-21
Findings	7: 4 Medium, 3 Low (all seven from the first notice, reassessed)
Status	NO REPLY AS OF 21 NOVEMBER 2026.
SHA-256 (base APK)	`7493eebdbc5fa0b46f407a84c331a5a0d444b96ed2618c4f9ca103dcdc1138cd`

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 Findings 6
- 5.1 C3: Racial and ethnic origin collected in a dedicated onboarding step, with no Art. 9 consent screen found . . . 6
- 5.2 C1: Firebase initializes at process start with data collection on by default, and a PostHog analytics client with named capture calls is bundled . . . 7
- 5.3 C2: Firebase API key hardcoded in res/values/strings.xml . . . 8
- 5.4 H3: No Art. 27 EU representative named for a US controller that addresses EEA, UK and Swiss residents . . . 9
- 5.5 H1: PEGI 3 rating against a policy that requires guardian consent under 18, with date of birth collected and no age check found . . . 10
- 5.6 H2: Recipients in the bundle that the Privacy Policy does not name: PostHog, TrainingPeaks, Google Translation and Geocoding . . . 11
- 5.7 M1: RECORD_AUDIO declared with no first-party audio feature found . . . 12

6 Impact Analysis 12

7 The Complete Chain 13

8 Special-Category Data & Bystanders 13

9 Data Protection: Article by Article 14

10 Regulatory & Legal Landscape 15

11 Indicators of Compromise & Reproducible Evidence 15

12 Disclosure Timeline & Outcome 16

13 What Nix Got Right 16

14 Residual Risk & Recommendations 17

Executive Summary

Nix Solo is the companion app of the Nix Hydration Biosensor, a sweat patch and pod that measure fluid and electrolyte loss during exercise. It is published on Google Play by Nix, Inc. of Norwell, Massachusetts, with 1K+ downloads. On 22 August 2026 RFI-IRFOS sent a coordinated disclosure notice under REF NIXSOLO-2026-R1 after a root level code analysis of version 3.44.3. It described three Critical and three High findings, one Medium, and asked three written questions.

Two findings carry the case. The app asks for the user's race in a dedicated onboarding step, a special category of personal data, and no consent screen for it was found in the package, while the operator's own Data Safety card declares the field as optional (C3). Firebase starts at process start with collection on by default, a PostHog analytics client is bundled, and no consent management platform exists, while the Data Safety card says no data is shared with third parties (C1).

The other findings are ordinary but real: a Firebase key is readable in the package, no EU representative is named, the PEGI 3 rating does not match the policy's guardian rule, the policy leaves out PostHog and TrainingPeaks, and a microphone permission has no visible purpose.

This report is stricter than the notice. All three Critical labels are reduced to Medium, the three High labels to Medium, Low and Low, and the Medium to Low, for the reasons given in each finding. Two statements of the notice are corrected. PostHog was said to initialize before any consent screen, which the package shows only for Firebase, and the absence of a consent mechanism for the race field was stated more firmly than a string search supports. Nix, Inc. has not replied to any message. The operator's Privacy Policy still reads May 2024, the Data Safety card still says no data is shared, and Google Play shows an app update on 10 November 2026 that this report did not analyse.

Scope: Root level code analysis of Nix Solo 3.44.3 (versionCode 3044003, package com.nixbiosensors), a 93.7 MB arm64-v8a XAPK bundle with a base.apk of 62,783,779 bytes: AndroidManifest.xml, decoded resources, 37,065 classes in five dex files counted from the dex headers, and the string pool of the Hermes JavaScript bundle assets/index.android.bundle. minSdk is 33 and targetSdk is 36. A full smali decompile was not run, so every statement that would need method bodies or screen flows is marked UNVERIFIED. The package came from the APKPure mirror because no audit device was connected, with package name, developer name and update date cross-checked against the live Google Play listing and the container hash matched against the mirror's published value. The operator's public Privacy Policy, the Google Play listing and the Data Safety card were read by plain HTTP GET, first on the analysis day and again for this report. The listing now shows an update on 10 November 2026, so the current build may differ from the audited one. No account was created, no Nix, Firebase or PostHog server was called and no key was tested. CVSS v4.0 measures exploitability. Most findings here are data-governance findings with no attacker, so the printed scores are low and two findings carry an explicit blast-radius escalation.

ID	Severity	Title
C3	MEDIUM	Racial and ethnic origin collected in a dedicated onboarding step, with no Art. 9 consent screen found
C1	MEDIUM	Firebase initializes at process start with data collection on by default, and a PostHog analytics client with named capture calls is bundled
C2	MEDIUM	Firebase API key hardcoded in res/values/strings.xml
H3	MEDIUM	No Art. 27 EU representative named for a US controller that addresses EEA, UK and Swiss residents
H1	LOW	PEGI 3 rating against a policy that requires guardian consent under 18, with date of birth collected and no age check found
H2	LOW	Recipients in the bundle that the Privacy Policy does not name: PostHog, TrainingPeaks, Google Translation and Geocoding
M1	LOW	RECORD_AUDIO declared with no first-party audio feature found

Finding Status at a Glance

ID	Disclosed	This report	Status on 14 November 2026
C3	CRITICAL	MEDIUM	No reply. Race field declared optional by the operator. Reassessed.
C1	CRITICAL	MEDIUM	No reply. PostHog timing narrowed. Reassessed.
C2	CRITICAL	MEDIUM	No reply. Key restrictions not examined. Reassessed.
H3	HIGH	MEDIUM	No reply. Live policy still names no representative.
H1	HIGH	LOW	No reply. Rating and policy still differ. Reassessed.
H2	HIGH	LOW	No reply. Reassessed.
M1	MEDIUM	LOW	No reply. Reassessed.

Subject & Operator Analysis

The operator is Nix, Inc., 354 Winter Street, Norwell, MA 02061, USA. Its only privacy contact in the policy is info@nixbiosensors.com, which is also the address the notice went to. The developer name on Google Play is Nix Biosensors. The Google Play listing shows 1K+ downloads.

Because the operator has no establishment in the Union, there is no lead supervisory authority under Art. 56 GDPR and each national authority is competent for its own residents. The Austrian Datenschutzbehörde and the European Data Protection Supervisor were copied on the first notice for transparency.

Architecture & Data Flow

- Platform: React Native app with a Hermes JavaScript bundle and Expo modules. minSdk 33, targetSdk 36.
- Device link: Bluetooth link to the Nix pod. CAMERA is used to scan the pod serial code with ML Kit.
- Onboarding: dedicated steps for race, gender identity and date of birth (C3, H1).
- Start-up: FirebaseInitProvider with initOrder 100, directBootAware and app_data_collection_default_enabled true (C1).
- Analytics: PostHog client with named capture calls and EU and US endpoints (C1).
- Integrations: TrainingPeaks OAuth, Google Translation and Geocoding (H2).
- Network configuration: no network_security_config.xml override, so the Android default blocks cleartext traffic on targetSdk 36.

What this report does not show is any payload that leaves the phone. Where a statement depends on it, the finding says UNVERIFIED.

Findings

C3: Racial and ethnic origin collected in a dedicated onboarding step, with no Art. 9 consent screen found

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), reassessed from CRITICAL in the first notice, rated MEDIUM by blast-radius escalation

The package contains a dedicated onboarding step for race, with named categories, next to steps for gender identity and date of birth. The operator's Privacy Policy lists race in the physiological profile it collects, and its Google Play Data Safety card lists "Race and ethnicity" under personal info. No stand-alone consent capture for this field was found in the package.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because the field is a special category, the operator's policy extends the same profile to medications and female health tracking, and the policy asserts an 18+ guardian-consent rule that the package does not enforce (H1). CRITICAL, as disclosed on 22 August 2026, is withdrawn because the operator declares the field optional, the Google Play listing shows 1K+ downloads, and the consent screen was not reconstructed.

```
boarding.race.title
boarding.race.reason
boarding.race.subtitle
boarding.race.white
boarding.race.hispanic
boarding.race.asian
boarding.race.next

boarding.gender.title / .reason / .male / .why
boarding.dob.title / .subtitle / .back / .next

auth.register.privacy_policy
auth.register.terms

Branco ou Caucasiano     (Portuguese value of one race option, recovered from the
    string pool)
```

Privacy Policy, "Last updated on May 14, 2024", verbatim: "physiological profile, including birthday, gender identity, race, weight, height, fitness/athlete level (e.g., professional or recreational)". The same list continues with "details submitted about diet, medications, and female health tracking".

Google Play Data Safety card, read during the preparation of this report: personal info "Name, Email address, and Race and ethnicity", with race and ethnicity marked "Optional" and the purpose "App functionality". Fitness info is listed under health and fitness.

Observed fact: race and ethnicity is collected by a dedicated onboarding step, the operator declares it as optional, and the only privacy strings at registration are the generic links auth.register.privacy_policy and auth.register.terms. Art. 9(1) GDPR lists racial or ethnic origin among the special categories and Art. 9(2)(a) allows processing on explicit consent. Not

shown: what the user sees on the race screen. The bundle is compiled Hermes bytecode, a string-pool search cannot rebuild the screen flow, and the content of boarding.race.reason was not recoverable. Whether the screen carries its own explicit consent, and whether it can be skipped, is UNVERIFIED. The first notice said that no mechanism anywhere in the code could lawfully collect the field. That sentence went further than the evidence. This report rates the finding MEDIUM, reassessed from the CRITICAL label of the first notice, because the field is declared optional by the operator and the absence of a consent screen is shown only by a string search.

GDPR: Art. 9(1), Art. 9(2)(a), Art. 5(1)(c), Art. 35

Impact: A person who sets up a hydration tracker is asked for their race, a category the law treats as especially sensitive, without any consent screen visible in the package. The policy also lists medications and female health tracking among the details a user may submit.

Fix: State on the race screen why the field is needed, ask for explicit and separate consent for it, keep it skippable, and add a Data Protection Impact Assessment for the special-category fields.

C1: Firebase initializes at process start with data collection on by default, and a PostHog analytics client with named capture calls is bundled

---

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 5.1 (CVSS-B), reassessed from CRITICAL in the first notice

FirebaseInitProvider is declared with initOrder 100 and directBootAware true, and the manifest sets app_data_collection_default_enabled to true. A ReactNativeFirebase provider with initOrder 99 sits beside it. The JavaScript bundle holds a PostHog project key and capture calls named after home-screen card swipes. No consent management marker exists in the resources or the bundle.

```
<provider android:authorities="com.nixbiosensors.firebaseinitprovider"
    android:directBootAware="true" android:exported="false"
    android:initOrder="100" android:name="com.google.firebase.provider.
    FirebaseInitProvider"/>
<provider android:authorities="com.nixbiosensors.reactnativefirebaseappinitprovider"
    android:exported="false" android:initOrder="99"
    android:name="io.invertase.firebase.app.ReactNativeFirebaseAppInitProvider"/>
<meta-data android:name="app_data_collection_default_enabled" android:value="true"/>
<meta-data android:name="firebase_messaging_auto_init_enabled" android:value="true"/>
```

```
phc_8YG425h2ebdM810IsvhDot4Ni4tzudxpjFlOhlsikUGG

posthog.capture("HOME SWEAT STATS CARD SWIPE")
posthog.capture("HOME INSIGHTS CARD SWIPE")
posthog.capture("HOME SWEAT PROFILE CARD SWIPE")

https://eu.i.posthog.com   https://eu-assets.i.posthog.com
https://us.i.posthog.com   https://us-assets.i.posthog.com
```

The trailing characters of the PostHog key are ambiguous under string-pool extraction from Hermes bytecode. The prefix phc_ and the body length match the standard PostHog project

key format. The value above is as extracted, and the final characters are UNVERIFIED.

Google Play Data Safety, read during the preparation of this report, verbatim: ”No data shared with third parties. The developer says this app doesn’t share user data with other companies or organizations.” The same card lists crash logs, diagnostics and device or other IDs for analytics.

Observed fact: Firebase starts when Android binds the process, before any consent screen can render, and the package has no consent management platform. The first notice said that PostHog also initializes before any consent screen. The package shows the capture calls and the project key. The point in the app lifecycle at which the PostHog client is created is a call-order question that the string pool cannot decide and is UNVERIFIED. The bundle contains SDK strings about session replay (”Session replay SDK config”, ”Session replay enabled but not installed.”). They are SDK-internal messages and do not show that the replay plugin is installed or that replay is running. No recording was observed. The Data Safety statement and the policy are compared on the sharing question only at category level: Firebase and PostHog are analytics providers that plausibly act as processors, which Google’s form generally does not count as sharing. The first notice rated this CRITICAL. This report rates it MEDIUM because the evidence is a manifest fact and bundle strings, and no transmitted payload was observed.

GDPR: Art. 7(1), Art. 5(1)(a), Art. 5(2), Art. 13(1)(e), Art. 25, ePrivacy Directive Art. 5(3)

Impact: The app starts sending to Google’s analytics stack before the person can say anything about it, and a second analytics vendor sees which cards on their personal sweat profile they open.

Fix: Disable automatic Firebase initialization in the manifest, start Firebase and PostHog after the consent state is known, and align the Data Safety card with the analytics providers actually used.

C2: Firebase API key hardcoded in res/values/strings.xml

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N, 6.3 (CVSS-B), reassessed from CRITICAL in the first notice

The Firebase client configuration for project nix-solo-prod is readable from any copy of the package.

```
<string name="google_api_key">AIzaSyBDoF773K4t6M4CkZIu-UxrqjDpX8tFwRk</string>
<string name="google_app_id">1:726454950284:android:90c44b6c44945ed7469ea9</string>
<string name="google_storage_bucket">nix-solo-prod.firebasestorage.app</string>
<string name="project_id">nix-solo-prod</string>
<string name="gcm_defaultSenderId">726454950284</string>
```

Observed fact: Google documents Firebase API keys as project identifiers and every Firebase Android app carries one. The first notice listed five attack vectors, including absence of App Check and an unrestricted key. The package does not show the key restrictions, the App Check enforcement or the security rules of the project. No key was tested and no Google or Nix service was called, so all three are UNVERIFIED. The notice also tied the key to the safety value of real-time hydration alerts. Whether those alerts depend on the Firebase backend or run on the phone from the pod’s Bluetooth data is not shown by the package and is UNVERIFIED. The first notice rated this CRITICAL. This report rates it MEDIUM because

the key is public by design and the exposure depends on server-side settings that were not examined.

GDPR: Art. 32(1)(b), Art. 25

Impact: If the project is not locked down, anyone holding the key can use up its quota, which would interrupt the sync features of a sports app during a session.

Fix: Restrict the key to the package name and signing certificate and to the required APIs, enforce App Check, and review the security rules of project nix-solo-prod.

H3: No Art. 27 EU representative named for a US controller that addresses EEA, UK and Swiss residents

---

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), reassessed from HIGH in the first notice

Nix, Inc. is incorporated and headquartered in Norwell, Massachusetts. The app is available on the Austrian and EU Google Play store. The Privacy Policy has a dedicated section for residents of the EEA, the UK and Switzerland and sends every rights request to info@nixbiosensors.com, a US contact. No representative appears in the policy.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because the operator offers an app that collects special-category fields from EU residents and has no EU establishment, so the representative is the only local route for a data subject. HIGH, as disclosed on 22 August 2026, is withdrawn because the Google Play listing shows 1K+ downloads and the exemption of Art. 27(2) was not excluded.

Check against the live page, read during the preparation of this report: the Privacy Policy still reads "Last updated on May 14, 2024". The section "General Data Protection Regulation - GDPR" states that residents of Europe "may have additional rights" and that rights are exercised "by sending an email to info@nixbiosensors.com". The word representative appears only in the context of a "Managing Entity" of a coach or administrator. The page names no data protection officer and no legal basis.

Art. 27(1) GDPR requires a controller outside the Union that is subject to the GDPR under Art. 3(2) to designate a representative in writing. Art. 27(2)(a) exempts processing that is occasional, does not include large-scale special-category data and is unlikely to risk rights. An app that collects race and fitness data from every user is continuous processing, so the exemption is unlikely to apply, and its scale is UNVERIFIED. The Google Play listing shows 1K+ downloads.

Observed fact: no representative is named in the policy. Not shown: whether one has been designated elsewhere. The first notice rated this HIGH. This report rates it MEDIUM because the gap is a missing contact point and not a processing failure.

GDPR: Art. 27(1), Art. 13(1)(a), Art. 13(2)(d)

Impact: An EU resident who wants to ask what Nix holds about them must write to a US address. No EU contact is named.

Fix: Designate an Art. 27 representative in writing, name it with an EU address in the policy, and add the legal basis and the right to complain to a supervisory authority.

H1: PEGI 3 rating against a policy that requires guardian consent under 18, with date of birth collected and no age check found

LOW, CVSS v4.0 AV:N/AC:L/AT:P/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B), reassessed from HIGH in the first notice

The Google Play listing shows PEGI 3. The Privacy Policy states that individuals "under the age of 18 must do so with the express consent and approval of a legal guardian". The app collects date of birth in a named onboarding step.

```
boarding.dob.title
boarding.dob.subtitle
boarding.dob.back
boarding.dob.next

Searched with no match: too young, minimum_age, age_restrict, invalid_age, dob_error,
under_18, guardian, parent_consent, legal guardian
```

Observed fact: the PEGI rating and the policy do not match, and the string search found no age check tied to the date of birth. The bundle is compiled bytecode, so a check written with other wording would not be found, and the absence is UNVERIFIED. The mismatch is a labelling and design gap. It is not a processing finding by itself. The first notice rated it HIGH. This report rates it LOW because the harm is the rating label and the evidence of a missing check is a string search.

GDPR: Art. 8, Art. 25, Art. 5(1)(a)

Impact: A parent who relies on PEGI 3 would let a child install an app that asks for race and date of birth.

Fix: Add an age check tied to the date of birth, capture guardian consent where the policy requires it, and align the content rating with the policy.

H2: Recipients in the bundle that the Privacy Policy does not name: PostHog, TrainingPeaks, Google Translation and Geocoding

LOW, CVSS v4.0 AV:L/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.1 (CVSS-B), reassessed from HIGH in the first notice

The policy says that "Nix third party advertising and analytics partners include Google, Meta, and similar partners" and lists recipient categories. The bundle contains endpoints of PostHog, TrainingPeaks and two Google Cloud APIs.

```
https://eu.i.posthog.com , https://us.i.posthog.com                    PostHog
https://api.trainingpeaks.com , https://oauth.trainingpeaks.com
    TrainingPeaks, OAuth
https://translation.googleapis.com/language/translate/v2                 Google Cloud
     Translation
https://maps.googleapis.com/maps/api/geocode/json                        Google
    Geocoding, device pairing flow
```

Observed fact: Google is named in the policy, so the Translation and Geocoding calls fall under it. The Google calls use key placeholders substituted at runtime, so no additional key finding is made. PostHog is an analytics provider that "similar partners" covers only loosely. The TrainingPeaks integration is an OAuth link that the user starts to send workouts to a third-party platform, and transfers the user initiates are generally not what a Data Safety form counts as sharing. Art. 13(1)(e) asks for recipients or categories of recipients, and the policy gives categories. The first notice rated this HIGH. This report rates it LOW because the policy discloses categories, Google is named, and the TrainingPeaks link is user-initiated.

GDPR: Art. 13(1)(e), Art. 5(1)(a)

Impact: A user reading the policy learns that analytics partners exist, but not that a product-analytics vendor sees which cards they open.

Fix: Name PostHog and TrainingPeaks in the policy, and say that TrainingPeaks receives data only after the user connects an account.

M1: RECORD_AUDIO declared with no first-party audio feature found

LOW, CVSS v4.0 AV:L/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.1 (CVSS-B), reassessed from MEDIUM in the first notice

The manifest declares RECORD_AUDIO and CAMERA among 27 permissions. CAMERA has a demonstrated purpose, scanning the serial code of the Nix Pod at pairing with Google ML Kit barcode scanning. RECORD_AUDIO has no equivalent feature.

A second pass covered the string pool of the bundle and the strings of all five dex files for AudioRecord, MediaRecorder, audio classifier, spectrogram, mfcc and health-related audio features such as cough, breathing and sound environment. classes3.dex contains getMicrophonePermissionsAsync and requestMicrophonePermissionsAsync, which are stock Expo module functions. classes.dex contains AndroidX voice-search and media-session boilerplate. The spectrogram strings in the bundle sit inside the generic TensorFlow.js operation set. No Nix-specific audio feature was found.

Observed fact: a dangerous permission is declared without a demonstrated first-party purpose, and two benign library explanations fit. Not shown: whether any code path records audio. That is UNVERIFIED and no clean negative is claimed. The first notice rated this MEDIUM. This report rates it LOW because nothing indicates use.

GDPR: Art. 5(1)(c)

Impact: A user is asked to allow microphone access for an app whose visible functions do not need it.

Fix: Remove RECORD_AUDIO from the manifest if no feature uses it, or explain its purpose in the policy.

Impact Analysis

- Every user. Firebase starts before any choice is possible and a second vendor sees card interactions on the personal sweat profile (C1).
- Users who answer the race question. They give a special-category field with no visible consent screen in the package (C3).
- EU residents who want to exercise a right. They have no EU contact (H3).
- Parents. PEGI 3 does not match the policy’s guardian rule and the app asks for race and date of birth (H1).

Scale: the Google Play listing shows 1K+ downloads, which keeps the number of affected people small.

The Complete Chain

- 1. A person installs Nix Solo. At process start Firebase initializes with collection on by default (C1).
- 2. Onboarding asks for race, gender identity and date of birth. The package shows no consent screen for the race field (C3).
- 3. The home screen sends card interaction events to PostHog (C1).
- 4. The policy names Google and Meta and ”similar partners”. PostHog and TrainingPeaks are not named (H2).
- 5. The user wants to ask what is held. The policy sends the request to a US address (H3).
- 6. The notice asked three questions on 22 August 2026. No reply has arrived.

Each later section of this report refers to one of these six links. The harm is a processing chain that starts before the person can choose and has no EU contact.

Special-Category Data & Bystanders

Art. 9(1) GDPR lists racial or ethnic origin among the special categories, and Art. 9(2)(a) requires explicit consent. The policy extends the profile to ”diet, medications, and female health tracking”, which relate to health under Art. 4(15). Hydration and fitness data from a body sensor can also relate to health. Whether the operator’s combination of fields is large-scale processing under Art. 35(3)(b) is a question for its Data Protection Impact Assessment.

The Data Safety card marks race and ethnicity as optional. Optional collection helps the operator, since a user can decline, but it does not replace an explicit consent step for those who answer. No bystander data was found. The only camera use is scanning the pod’s serial code, and no audio feature was found.

Article	How it is engaged

Data Protection: Article by Article

Article	How it is engaged
Art. 5(1)(a)	Transparency. Data Safety card and policy on recipients (C1, H2).
Art. 5(1)(c)	Data minimisation. Race field and microphone permission (C3, M1).
Art. 5(2)	Accountability. A design with no consent management platform (C1).
Art. 7	Consent. Firebase starts before any choice (C1).
Art. 8	Age of the user. PEGI 3 and the guardian rule (H1).
Art. 9(1), 9(2)(a)	Racial or ethnic origin, and health-related profile fields (C3).
Art. 13(1)(a), 13(1)(e), 13(2)(d)	Controller contact, recipients, right to complain (H2, H3).
Art. 25	Data protection by design and by default (C1, H1).
Art. 27	EU representative (H3).
Art. 32(1)	Security of processing. Client key (C2).
Art. 33(4)	Raised in the notice so the timeline is clear. No breach is asserted.
Art. 35	DPIA for the special-category fields (C3).
ePrivacy Directive Art. 5(3)	Access to information on the terminal device (C1).

Regulatory & Legal Landscape

A US operator with no Union establishment answers to each national supervisory authority for its residents and must have an Art. 27 representative where Art. 3(2) applies, unless the Art. 27(2) exemption holds. The Datenschutzbehörde and the EDPS were informed for transparency. Research on the published package is protected by Art. 17 StGG and follows ISO/IEC 29147.

Industry comparison: a stand-alone consent screen for special-category fields, a named representative with an EU address, and analytics that start only after consent are the usual pattern for health and fitness apps offered in the EU. The CCPA supplement in the policy is more detailed than the GDPR section.

Indicators of Compromise & Reproducible Evidence

Every point below can be reproduced from the public package and the public web pages. The package came from the APKPure mirror. The container hash matches the value published by the mirror. The signer certificate hash is the value reported by the mirror.

```
Package       com.nixbiosensors
Version       3.44.3 / versionCode 3044003 (analysed 2026-08-22)
base.apk      SHA-256 7493eebdbc5fa0b46f407a84c331a5a0d444b96ed2618c4f9ca103dcdc1138cd
XAPK bundle   SHA-256 69f753934b7c5c92ddf10f5ae9aad5012811eac005abe5208759df3db72840bc
Signer cert   SHA-1 0ab9c89c7ddefc3b3d8a34b32a58a356d19a520b (reported by APKPure)
Firebase      project nix-solo-prod, app 1:726454950284:android:90c44b6c44945ed7469ea9
              google_api_key AIzaSyBDoF773K4t6M4CkZIu-UxrqjDpX8tFwRk
              bucket nix-solo-prod.firebasestorage.app, sender 726454950284
PostHog       phc_8YG425h2ebdM810IsvhDot4Ni4tzudxpjFlOhlsikUGG (trailing characters
    ambiguous)
```

```
https://nixbiosensors.com/pages/privacy-policy
https://play.google.com/store/apps/details?id=com.nixbiosensors
https://play.google.com/store/apps/datasafety?id=com.nixbiosensors
https://eu.i.posthog.com , https://us.i.posthog.com
https://api.trainingpeaks.com , https://oauth.trainingpeaks.com
```

```
Operator contact  info@nixbiosensors.com
Copied           dsb@dsb.gv.at, edps@edps.europa.eu
```

Disclosure Timeline & Outcome

Date	Event
2026-08-22	Analysis of version 3.44.3. Notice REF NIXSOLO-2026-R1 sent to info@nixbiosensors.com, copied to the Datenschutzbehörde and the EDPS. Three written questions. A reply was asked for by 4 September 2026.
2026-09-05	Follow-up on the same thread. Findings restated unchanged. Answers requested by 19 September 2026.
2026-10-17	Reminder, 35 days before publication. Three questions unchanged.
2026-11-14	No reply of any kind and no bounce received for any message.
2026-11-21	Publication date announced in every message.

The operator received the same embargo date in every message. No request to extend it was made and none was granted.

What Nix Got Right

- No cleartext traffic override exists, so the Android default of blocking cleartext HTTP holds on targetSdk 36.
- The Data Safety card lists race and ethnicity as collected data, marks it optional and does not hide it.
- CAMERA maps to one narrow, demonstrated purpose, scanning the pod serial code.
- The endpoint inventory shows no SDK from a sanctioned or high-risk jurisdiction. The stack is Google, PostHog and TrainingPeaks.
- The policy has a dedicated GDPR section and a detailed CCPA supplement that states Nix does not sell personal data.

Residual Risk & Recommendations

All seven findings are open. No reply has been received. Versions after 3.44.3 are not covered by this report, and Google Play shows an update on 10 November 2026.

- Put an explicit consent step on the race screen, keep the field skippable and run a Data Protection Impact Assessment.
- Start Firebase and PostHog after the consent state is known.
- Restrict the Firebase key and enforce App Check.
- Designate an Art. 27 representative and name it in the policy.
- Add an age check tied to the date of birth, name PostHog and TrainingPeaks in the policy and remove RECORD_AUDIO if unused.
- Answer the three written questions.

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 operator’s public Privacy Policy and Google Play pages. No Nix, Firebase or PostHog servers or accounts were probed and no key was tested. Severity per CVSS v4.0 (CVSS-B) with explicit blast-radius escalation where stated. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. RFI-IRFOS, ZVR 1015608684, GISA 39261441. REF NIXSOLO-2026-R1.