Security & Privacy Disclosure, Final Report

Willow (com.willow.go)

A health app that starts Firebase before any screen, a dialog about pumping tips that primes an advertising permission, and no reply to three questions.

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

Target	Willow Innovations, Inc. (Play Store developer entity EXPLORAMED NC7, LLC)
Versions Audited	4.3.6 / 479 (analysis 2026-08-22)
Notice / Publication	2026-08-22 / 2026-11-20 (90 days)
Findings	6: 3 Medium, 1 Low, 2 observations (five disclosed severities reassessed in this report)
Status	NO REPLY OF ANY KIND AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`244500171841b98de2c32155142380a8712b7e24b6dddfd19d29d1fb5a67e2c7`

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 Applicability of GDPR, Stated First 4

3 Finding Status at a Glance 5

4 Subject & Operator Analysis 5

5 Architecture & Data Flow 6

6 Engagement Summary 7

7 Findings 8

7.1 C1: Firebase starts before any screen and before unlock, Firebase not named in the policy . . . 8

7.2 H1: Advertising ID permission requested through a dialog about pumping tips . 9

7.3 H2: Firebase and Braze keys and the production project configuration in strings.xml . . . 10

7.4 M1: No network security configuration and no certificate pinning . . . 11

7.5 M2: Google Play names EXPLORAMED NC7, LLC as developer, the Privacy Notice names Willow Innovations, Inc. . . . 12

7.6 O1: In-app chat disclaimer calls data anonymous, the message endpoint sits behind a per-user API . . . 13

8 Impact Analysis 13

9 The Complete Chain 14

10 Consumer Protection & Platform Disclosures 14

11 Data Protection: Article by Article 15

12 Regulatory & Legal Landscape 15

13 Indicators of Compromise & Reproducible Evidence 16

14 Disclosure Timeline & Outcome 16

15 What Willow Got Right 17

16 Residual Risk & Recommendations 17

Executive Summary

Willow is the companion app for wearable in-bra breast pumps. It controls the pump, logs pumping sessions, tracks milk bags and offers an AI chat for maternal health questions. On 22 August 2026 RFI-IRFOS sent a notice under REF WILLOW-2026-R1, based on a root level code analysis of version 4.3.6, to the support and developer addresses, with the Datenschutzbehörde and the European Data Protection Supervisor in copy.

One fact shapes every legal statement in this report. RFI-IRFOS cannot establish that GDPR applies to this operator. The app is region-locked, the operator's Privacy Notice covers Canada, the United States and several US states and has no EU or EEA section, and the notice itself asked the operator whether it considers itself in scope. The technical facts hold under any law, and the GDPR articles are cited as conditional.

The lead finding is structural. Firebase starts through a manifest ContentProvider before any screen and before device unlock, with 27 component registrars that cover Firestore, Auth, Analytics and Crashlytics. The operator's Privacy Notice of 2023 calls pumping history, delivery method and mood or sleep sensitive personal information, names Braze fifteen times and does not name Firebase. A dialog titled Personalize your pumping experience introduces the system prompt for the advertising ID without naming advertising. Firebase and Braze keys and the production project configuration ship in the package. The people affected are parents in the first weeks and months after birth.

Willow has not replied. The mailbox holds no answer, no automatic reply and no delivery failure notice for the notice, two follow-ups of 12 September and one follow-up of 17 October 2026. This report separates what the package shows from what only the operator can say. Compared with the notice, five severities are lower here, one of them as an observation, and the Dart code that holds the consent flow was not disassembled.

Scope: Root level code analysis of the Google Play release 4.3.6 (versionCode 479) as an XAPK from a download mirror, with the live Google Play listing and the Privacy Notice read on 22 August 2026. Resources were decoded without sources and classes.dex and libapp.so were searched for class descriptors, endpoints and strings. The Dart snapshot was not disassembled. No backend was contacted, the keys were not tested 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	Firebase starts before any screen and before unlock, Firebase not named in the policy
H1	MEDIUM	Advertising ID permission requested through a dialog about pumping tips
H2	MEDIUM	Firebase and Braze keys and the production project configuration in strings.xml
M1	LOW	No network security configuration and no certificate pinning
M2	INFO	Google Play names EXPLORAMED NC7, LLC as developer, the Privacy Notice names Willow Innovations, Inc.
O1	INFO	In-app chat disclaimer calls data anonymous, the message endpoint sits behind a per-user API

Applicability of GDPR, Stated First

RFI-IRFOS cannot establish from the evidence gathered that GDPR territorial scope under Article 3(2) applies to this operator. The app is region-locked. It returned "This app is not available for any of your devices" from an Austrian Play Store session. The operator's Privacy Notice has a Region-Specific Disclosures section for Canada, the United States, Nevada, Colorado, Connecticut, Utah, Virginia and California and contains no EU, EEA or United Kingdom section. The terms GDPR, European, EEA and Data Protection Officer do not occur in it. This is consistent with public reporting that the product is sold in the United States and Canada, a statement that was not re-verified for this report.

The GDPR articles in this report are cited because they are the standing framework of the institute, and each applies only if the regulation is engaged. The technical facts, the pre-consent Firebase start, the keys and the wording of the dialog, are true under any law. The operator's own notice acknowledges the California Consumer Privacy Act and the California Privacy Rights Act, and the Nevada, Colorado, Connecticut, Utah and Virginia statutes, so a parallel set of duties exists in any case. Question 1 of the notice asks the operator directly whether it considers itself in scope.

Finding Status at a Glance

The table shows the severity named in the notice of 22 August 2026 next to the severity in this report. Five labels differ. Every change follows from the evidence as described in the Basis column. No label changed because of a statement by Willow, which has not replied. The notes recorded one further candidate, the Ema chat disclaimer, which appears here as O1.

ID	Notice	This report	Basis
C1	CRITICAL	MEDIUM	CVSS 6.9. Structural sequence documented, data flow and consent layer not observed, GDPR scope not established.
H1	HIGH	MEDIUM	CVSS 2.1, raised one band by blast-radius escalation. Wording documented, runtime flow not observed.
H2	HIGH	MEDIUM	CVSS 6.3. Key exposure, App Check registered, rules not examined.
M1	MEDIUM	LOW	CVSS 2.3. Pinning absent, cleartext denied by default.
M2	MEDIUM	INFO	Naming difference documented, relationship unverified.
O1	candidate	INFO	Wording and endpoint documented, anonymity basis unverified.

Subject & Operator Analysis

Willow (package com.willow.go) is the companion app for the operator’s wearable in-bra breast pumps (Willow Go, Willow Sync, Willow 360, Willow 3.0). The app controls the pump over Bluetooth, logs pumping sessions and milk output, manages a digital milk bag inventory (SmartStash) with barcode or QR scanning, and offers an AI chat feature named Ema for maternal health questions. The Play listing shows 10K+ downloads, category Health and Fitness, rating PEGI 3 and an update on 29 June 2026. A second package, com.willowpump.willow (Willow Gen 3), returned a not-found page on 22 August 2026 and was not analysed.

The consumer brand and the Play Store headline developer is Willow Innovations, Inc. The developer transparency panel names EXPLORAMED NC7, LLC, Mountain View, California. The relationship between the two is UNVERIFIED. No data protection officer and no representative in the Union under Article 27 was found in the binary, the Play listing or the Privacy Notice, which is consistent with the applicability question above. No EU main establishment is evidenced anywhere in the material. If GDPR applied, each concerned authority would be competent, and for an Austrian matter that is the Datenschutzbehörde.

Item	Value
Package	com.willow.go
Version	4.3.6 (versionCode 479), minSdk 29, targetSdk 36

Item	Value
base APK SHA-256	244500171841b98de2c32155142380a8712b7e24b6dddfd19d29d1fb5a67e2c7
XAPK SHA-256	574f4db6fd22fb64c9bc728da69d3f82dc3a91cc0f5772bd42da33cb70bfbf69
Signing certificate SHA-1	eca33432d06900424f32eb5ca8dce58ffdc4b362 (Google Play App Signing, verified with apksigner, matches the value published by the mirror)
Size	XAPK 45.7 MB (base APK 18.7 MB, arm64 split 26.9 MB)
Code base	Flutter and Dart. Business logic is AOT-compiled to lib/arm64-v8a/libapp.so (16.0 MB), engine libflutter.so (10.8 MB), one classes.dex (8.6 MB) with the platform channel layer: Firebase, Braze, AndroidX, Google Play Services, CameraX
Source of the package	Download mirror, signature checked against the mirror's published value. The app was not installed on the audit device
Contacts	care@onewillow.com (support), appdev@onewillow.com (developer contact), https://onewillow.com/privacy-notice/

Architecture & Data Flow

Resources were decoded without sources (apktool with no smali). Raw byte-pattern searches covered classes.dex and libapp.so for class descriptors, endpoints and string constants. No baksmali, no jadx and no disassembly of the Dart snapshot 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
Pump link	Bluetooth control of the pump, WebSocket transport over wss to wss.wiapis.com	Manifest, strings
Backend	Firebase project wi-prod with Analytics, Auth, Crashlytics, Remote Config, Storage, Firestore, Messaging, Sessions, Installations, App Check, A/B Testing. REST-style /users/{userId}/ endpoints on hello.onewillow.com	Manifest, libapp.so strings
Engagement	Braze SDK, endpoint sdk.iad-02.braze.com (US East)	strings.xml
Advertising	AD_ID and ACCESS_ADSERVICES permissions, Google Ads conversion and deep-link endpoints, no mediation network	Manifest, classes.dex
Camera	CameraX recording with audio for barcode scanning of the milk bag feature, no audio analysis markers	classes.dex

Layer	Observed	Source
AI chat	Ema, /ema/message/{conversationId}	Strings
Consent	No consent management platform found. Dart interface layer not inspected	Dex and libapp.so search
Billing	No billing permission, no purchase library, no paid version in the Android binary	Manifest, dex

Engagement Summary

The notice went on 22 August 2026 at 12:49 UTC to care@onewillow.com and appdev@onewillow.com, with the Datenschutzbehörde and the European Data Protection Supervisor in copy. It said in its first lines that GDPR scope could not be confirmed. It named C1, H1 and H2 in full, summarised the two further findings, set out three questions, asked for a reply in writing within 30 days with a named contact, and announced publication after a 90-day embargo from delivery, which gives 20 November 2026. Two follow-ups went on 12 September 2026 and one on 17 October 2026. No message from Willow of any kind is in the mailbox as of 14 November 2026. No automatic reply and no delivery failure notice arrived for any of the four messages.

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

Findings

C1: Firebase starts before any screen and before unlock, Firebase not named in the policy

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". Android instantiates a manifest ContentProvider during application creation, before any Activity can render a consent screen, and a directBootAware component can run before the device is unlocked. The ComponentDiscoveryService registers 27 Firebase component registrars that resolve to Analytics, Auth, Crashlytics, Remote Config, Storage, Firestore, Messaging, Sessions, Installations, App Check and A/B Testing. Firestore is the app's primary database, evidenced by /users/{userId}/... REST-style Dart model classes in libapp.so. The operator's Privacy Notice (https://onewillow.com/privacy-notice/, effective 1 January 2023) states: "In the last 12 months, we have collected the following categories of sensitive personal information: Health Information, such as delivery method (i.e., natural or C-section), your pumping history, and how you are generally feeling (i.e., your mood or how are you sleeping)." That notice names Braze fifteen times and does not name Firebase or Crashlytics. What Firebase transmits, and whether a consent step exists in the Dart interface layer, were not observed. The finding is the structural sequence and the disclosure gap, set in the frame stated on the first page: GDPR territorial scope is not established for this operator. 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.willow.go.firebaseinitprovider" android:
    directBootAware="true" an
    droid:exported="false" android:initOrder="100" android:name="com.google.firebase.
    provider.Fireba
    seInitProvider"/>
<service android:directBootAware="true" android:exported="false" android:name="com.
    google.firebase.c
    omponents.ComponentDiscoveryService">
    27 registered component registrars, among them AnalyticsConnectorRegistrar,
    CrashlyticsRegistrar
    , FirestoreRegistrar, FirebaseSessionsRegistrar
<service android:directBootAware="true" android:exported="false" android:name="com.
    google.firebase.m
    essaging.FirebaseMessagingService">
```

```
UsersUserIdBagsPatchRequest
UsersUserIdLocationsLocationIdPatchRequest
UsersUserIdBricksPostRequest
```

A consent-management search (OneTrust, Didomi, Usercentrics, consentmanager) returned no hit in classes.dex and libapp.so. The IABTCF constants that exist are boilerplate from a Google Play Services dependency and are not evidence of an active consent implementation. Whether a custom consent screen exists inside the Dart interface layer is UNVERIFIED,

because Dart compiled to ARM64 machine code was not disassembled.

Impact: The people affected are parents who log pumping history, delivery method and mood or sleep, data that the operator's own notice calls sensitive, in an app whose backend provider is not named in that notice.

Fix: Name Firebase and Crashlytics with their purposes in the Privacy Notice, state which technical measure starts Firebase only after a documented consent step where one is required, and date the notice currently.

H1: Advertising ID permission requested through a dialog about pumping tips

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 manifest declares com.google.android.gms.permission.AD_ID, ACCESS_ADSERVICES_ATTRIBUTION, ACCESS_ADSERVICES_AD_ID and the Play Install Referrer permission. classes.dex holds two Google Ads endpoint strings of the standard conversion and deep-link type, keyed by the advertising ID. The in-app translation file holds the dialog that precedes the system prompt, with the header "Personalize your pumping experience" and the body "We're thrilled you've chosen us to be part of your breastfeeding journey. Please choose "Allow" on the next screen to get personalized pumping tips". The dialog names no advertising, no tracking and no third party. The key names dialog-app-tracking-header and dialog-app-tracking-body show what the dialog introduces. The capability and the framing are in the package. The runtime destination and payload of the advertising ID after a grant were not observed. RFI-IRFOS blast-radius escalation: raised from LOW/2.1 to MEDIUM because the consent request is addressed to people in the first weeks postpartum and its wording, quoted verbatim, names a feeding feature and not advertising.

```
com.google.android.gms.permission.AD_ID
android.permission.ACCESS_ADSERVICES_ATTRIBUTION
android.permission.ACCESS_ADSERVICES_AD_ID
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE
com.google.android.providers.gsf.permission.READ_GSERVICES
```

```
https://www.googleadservices.com/pagead/conversion/app/deeplink?id_type=adid&sd...
https://pagead2.googlesyndication.com/pagead/gen_204?i...
```

```
"dialog-app-tracking-header": "Personalize your pumping experience",
"dialog-app-tracking-body": "We're thrilled you've chosen us to be part of your
    breastfeeding journe
    y. Please choose \"Allow\" on the next screen to get personalized pumping tips",
```

Impact: The people addressed are parents in the first weeks and months after birth, asked to tap Allow for a feeding feature, with a system prompt that follows and a permission that serves advertising attribution.

Fix: Name the use of the advertising ID in the dialog in plain words, separate it from the pumping features, and state what the identifier is sent to.

H2: Firebase and Braze keys and the production project configuration in strings.xml

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

The values below ship in every copy of version 4.3.6. Firebase API keys and Braze SDK keys are not secrets by their vendors' design. The finding concerns availability: quota and billing exhaustion against the production project wi-prod, or against the Braze integration, until session sync, push reminders and milk bag inventory sync go offline. The notice also named unrestricted-key replay against other Google APIs if the key carries no package restriction, project and IAM enumeration, and an unauthenticated file server if the storage bucket rules are open. The key was not tested and no rules were examined. Firebase App Check is registered (FirebaseAppCheckRegistrar), which reduces but does not remove the exposure, and a shipped key cannot be rotated for installed copies without an app update. The Braze endpoint sdk.iad-02.braze.com resolves to the vendor's US East region. It was disclosed as HIGH on 22 August 2026 and is reassessed in this report to the band of its vector.

```
<string name="google_api_key">AIzaSyA-KpsTzV-rcUMV1bqf7XMzSN10mcmBrg0</string>
<string name="google_crash_reporting_api_key">AIzaSyA-KpsTzV-rcUMV1bqf7XMzSN10mcmBrg0
    </string>
<string name="google_app_id">1:834859049579:android:96327dfb836836496cc72e</string>
<string name="project_id">wi-prod</string>
<string name="google_storage_bucket">wi-prod.appspot.com</string>
<string name="gcm_defaultSenderId">834859049579</string>
<string name="default_web_client_id">834859049579-a06tos33te7cgs4go3ugv1i5bs05cdp2.
    apps.googleuserco
    ntent.com</string>
<string name="com_braze_api_key">049ac223-e0fd-46a5-97b8-995e3c33f591</string>
<string name="com_braze_custom_endpoint">sdk.iad-02.braze.com</string>
```

Impact: The direct exposure is the availability of the operator's production backend for parents who rely on session sync and reminders. Exposure of stored data would depend on rules that the operator can confirm.

Fix: Restrict the Firebase key by package name and signing certificate, confirm deny-by-default rules for Firestore and Storage, and confirm rate limits on the Braze integration.

M1: No network security configuration and no certificate pinning

LOW, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B), disclosed as MEDIUM on 22 August 2026, reassessed in this report

The application element declares no android:networkSecurityConfig, and res/xml holds only flutter_image_picker_file_paths.xml, flutter_share_file_paths.xml, image_share_filepaths.xml and splits0.xml. Because targetSdkVersion is 36, the platform default denies cleartext traffic. No certificate pinning exists for the operator's hosts (hello.onewillow.com, wss.wiapis.com) or for third-party endpoints, so the TLS channel relies on the system trust store. The pump communication backend is reached over wss, which is encrypted. A hostile certificate authority on the device is the route to interception. It was disclosed as MEDIUM on 22 August 2026 and is reassessed in this report to the band of its vector.

```
AndroidManifest.xml: no android:networkSecurityConfig
res/xml/: flutter_image_picker_file_paths.xml, flutter_share_file_paths.xml,
    image_share_filepaths.x
    ml, splits0.xml
Hosts: hello.onewillow.com, wss.wiapis.com
```

Impact: The exposure is limited to a network attacker who controls a trusted certificate authority on the device. Pump session data and self-declared sensitive health data travel over that channel.

Fix: Add pinning for the operator's API and WebSocket hosts or document why system trust is accepted.

M2: Google Play names EXPLORAMED NC7, LLC as developer, the Privacy Notice names Willow Innovations, Inc.

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

The Play Store headline developer is Willow Innovations, Inc. The developer transparency panel names EXPLORAMED NC7, LLC, 1975 W El Camino Real Ste 306, Mountain View, CA 94040, United States, with appdev@onewillow.com and +1 401-400-2125. The Privacy Notice carries the copyright line "©2023 Willow Innovations, Inc." and does not mention ExploraMed. Neither the in-app strings nor the notice identify the entity in the panel or explain its relationship to the brand entity. No wrongdoing is asserted. The relationship between the two entities is UNVERIFIED. The item matters because a person who wants to exercise a rights request needs to know which entity controls the listing. It is recorded as an observation because a documented naming difference does not carry a CVSS score. It was disclosed as MEDIUM on 22 August 2026.

```
Play Store headline developer:     Willow Innovations, Inc.
Play Store About the developer:   EXPLORAMED NC7, LLC
                                  1975 W El Camino Real Ste 306, Mountain View, CA
    94040, United Sta
    tes

                                  appdev@onewillow.com, +1 401-400-2125
Privacy Notice copyright line:    "©2023 Willow Innovations, Inc." (ExploraMed not
    mentioned)
```

Impact: A parent who wants to ask for access or deletion cannot tell from the notice which legal entity to address.

Fix: State in the Privacy Notice which entity is the controller and how it relates to the Play Store developer.

O1: In-app chat disclaimer calls data anonymous, the message endpoint sits behind a per-user API

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

The in-app AI chat feature Ema carries a disclaimer that reads: ”all data collected is encrypted and anonymous, so it cannot be directly associated with you”. The chat endpoint (/ema/message/{conversationId}) sits behind the same authenticated /users/{userId} API structure as pump and inventory data. The package shows the wording and the endpoint structure. How anonymity is established, and what is stored per conversation, is UNVERIFIED. The item was a candidate in the findings notes and the notice asked about it as part of question 3. It is recorded as an observation.

```
Disclaimer text: "all data collected is encrypted and anonymous, so it cannot be
    directly associated
     with you"
Endpoint string: /ema/message/{conversationId}
```

Impact: A parent who types a question about her health into the chat reads that it cannot be linked to her, while the technical structure shown is account-bound.

Fix: Explain the technical basis of the anonymity claim or correct the disclaimer.

Impact Analysis

The people in the path of these mechanisms are parents who use a pump companion app in the first weeks and months after birth. They log pumping history, delivery method, mood and sleep in an app whose Privacy Notice calls that data sensitive and does not name the backend provider that processes it. They are asked to allow advertising-attribution tracking through a dialog about pumping tips. Their questions to an AI chat feature are described as anonymous.

Whether any of this falls under GDPR is not established. Under the operator’s own acknowledged California and other state laws, the same disclosure gaps are relevant.

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 parent installs the companion app and pairs the pump	Play listing, manifest	All
Firebase starts before any screen and before unlock	Manifest, directBootAware, initOrder 100	C1
The parent sees a dialog about pumping tips, then the system advertising prompt	en-US.json, AD_ID permissions	H1
Health entries go to Firestore and engagement data to Braze US East	Strings, endpoints	C1, H2
The Privacy Notice dated 2023 names Braze and does not name Firebase	Privacy Notice, read 2026-08-22	C1
The operator has not answered the three questions	Thread, 22 Aug to 17 Oct 2026	All

The weak link of the chain is the same in C1 and H1: the package shows what is built and what the dialog says, and only the operator can say what is sent and under which law.

Consumer Protection & Platform Disclosures

The app is free companion software for hardware that the user already owns. The Android binary has no billing permission and no purchase library, so no paying customer is tracked like a free one here.

The Play listing names a developer entity that the Privacy Notice does not name (M2). The content rating is PEGI 3. The tracking dialog (H1) is a consumer protection question under any law, because its text frames an advertising permission as a feeding feature.

Data Protection: Article by Article

Every article below applies only if GDPR is engaged, which is not established. The column Finding shows where the facts sit.

Article	Relevance	Finding
3(2)	Territorial scope: offering to or monitoring people in the Union, open	All
4(7), 13(1)(a)	Identity of the controller	M2
5(1)(a)	Transparency: Firebase not named, dialog wording, anonymity claim	C1, H1, O1
6(1), 7(1), 7(2)	Legal basis, consent before processing, consent request in plain language	C1, H1
13(1)(e)	Recipients: Firebase and Crashlytics absent from the notice	C1
25, 32(1)(a), (b)	Design, pinning, exposed keys	H2, M1

Regulatory & Legal Landscape

If GDPR applies, the bases are Regulation (EU) 2016/679 Articles 3, 4, 5, 6, 7, 13, 25 and 32. The operator is established in the United States and no EU establishment is evidenced, so Article 3(2) is the only route and the question was put to the operator. Without a main establishment in the Union, each concerned authority would be competent. The Datenschutzbehörde (dsb@dsb.gv.at) and the European Data Protection Supervisor (edps@edps.europa.eu) were in copy of the notice of 22 August 2026, and the European Data Protection Supervisor of the second follow-up of 12 September 2026.

The operator’s own Privacy Notice names the California Consumer Privacy Act and California Privacy Rights Act (Cal. Civ. Code 1798.100 et seq.) and the Nevada, Colorado, Connecticut, Utah and Virginia statutes. 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 report makes no comparison with other applications.

Indicators of Compromise & Reproducible Evidence

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

```
Package       com.willow.go 4.3.6 (479)
base APK      244500171841b98de2c32155142380a8712b7e24b6dddfd19d29d1fb5a67e2c7
XAPK          574f4db6fd22fb64c9bc728da69d3f82dc3a91cc0f5772bd42da33cb70bfbf69
Signer SHA-1  eca33432d06900424f32eb5ca8dce58ffdc4b362
Firebase      project wi-prod, bucket wi-prod.appspot.com, sender 834859049579
API key       AIzaSyA-KpsTzV-rcUMV1bqf7XMzSN10mcmBrg0
App ID        1:834859049579:android:96327dfb836836496cc72e
Web client    834859049579-a06tos33te7cgs4go3ugv1i5bs05cdp2.apps.googleusercontent.com
Braze         key 049ac223-e0fd-46a5-97b8-995e3c33f591, endpoint sdk.iad-02.braze.com
Provider      com.willow.go.firebaseinitprovider (initOrder 100, directBootAware)
Hosts         hello.onewillow.com, wss.wiapis.com
Ads           googleadservices.com/pagead/conversion/app/deeplink, pagead2.
    googlesyndication.com/pag
    ead/gen_204
Policy        https://onewillow.com/privacy-notice/ (effective 2023-01-01)
Contacts      care@onewillow.com, appdev@onewillow.com
```

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

Disclosure Timeline & Outcome

Date	Event
22 Aug 2026	Notice REF WILLOW-2026-R1 at 12:49 UTC to care@onewillow.com and appdev@onewillow.com, Datenschutzbehörde and EDPS in copy. GDPR scope stated as unconfirmed, three questions, reply requested within 30 days, publication after a 90-day embargo from delivery.
12 Sep 2026	12:58 UTC first follow-up: no reply of any kind after 21 days, the three questions repeated, answer requested by 19 September 2026. 12:59 UTC second message in the older thread subject, EDPS in copy.
17 Oct 2026	Follow-up 34 days before publication, 56 days after the notice, to both addresses.
14 Nov 2026	No message from Willow. No automatic reply and no delivery failure notice for any of the four messages.
20 Nov 2026	Publication date, unchanged since 22 August 2026.

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

What Willow Got Right

No advertising mediation network is embedded. The advertising surface is limited to Google Ads attribution. No Chinese or sanctioned-jurisdiction SDK was found in classes.dex or libapp.so, checked in both. The two apparent hits (mbridge and umeng) were traced to time zone and locale data and are false positives. RECORD_AUDIO traces to the CameraX recording path for barcode scanning, and no audio analysis marker was found. Firebase App Check is registered. allowBackup is false and targetSdkVersion is 36, so cleartext traffic is denied by default. The WebSocket transport uses wss. The Privacy Notice names Braze fifteen times, so third-party processors are disclosed as a category and the gap is Firebase specifically. The analysed file is an authentic Play-distributed build, checked with apksigner.

Residual Risk & Recommendations

Priority	Action	Finding
1	State which entity is the controller and whether the operator considers the product in scope of GDPR	M2
2	Name Firebase and Crashlytics in the Privacy Notice and date the notice currently	C1
3	Describe the technical measure that starts Firebase only after a documented consent step where one is required	C1
4	Rewrite the tracking dialog to name the use of the advertising ID	H1
5	Explain the anonymity claim of the chat feature or correct it	O1
6	Restrict the Firebase key, confirm rules and Braze limits	H2
7	Pin the API and WebSocket hosts	M1

Residual risk: the Dart code that holds the consent flow, the chat storage and the dialog logic was not disassembled. This report describes version 4.3.6 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 Notice. No backend was contacted and the keys were not tested. GDPR articles apply only if the regulation is engaged. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Arts. 3, 4, 5, 6, 7, 13, 25, 32. RFI-IRFOS ZVR 1015608684, GISA 39261441. REF WILLOW-2026-R1.