# Security & Privacy Disclosure, Final Report

## Oticon Companion for Android (com.oticon.app)

A hearing aid app that calls hearing data sensitive in its support flow and anonymous on the switch that collects the most of it.

**PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO DATE 20 NOVEMBER 2026 REACHED. ONLY AN AUTOMATED TICKET ACKNOWLEDGEMENT, NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026.**

| | |
|---|---|
| **Target** | Oticon A/S, Smørum, Denmark (Demant A/S brand, platform OneApp) |
| **Versions Audited** | 1.8.0 / 617548 (2026-08-22) |
| **Notice / Publication** | 2026-08-22 / 2026-11-20 (90 days) |
| **Findings** | 5: 1 High, 3 Medium, 1 Low |
| **Status** | Automatic acknowledgement only, no substantive reply as of 21 November 2026. |
| **SHA-256 (base APK)** | `acc8f305dab947806e997c989c6759e00b2d6bbf49589fe1efe43a69b722c767` |

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 6

6 Findings 7

6.1 H1: Hearing aid data is called sensitive personal data related to hearing health in the support flow, and the consent switch that gates wearing time tracking calls it anonymous data . . . 7

6.2 M1: An authorization key for the production backend api.demant.com is stored in plain text in the app configuration . . . 8

6.3 M2: Firebase and Maps keys of the shared OneApp project oneapp-prod-13d7a are stored in plain text . . . 9

6.4 M3: PACKAGE_USAGE_STATS and READ_PHONE_STATE are declared and the package shows no feature that uses them . . . 10

6.5 L1: No age verification is visible in the package, registration runs in a hosted flow, and the PEGI 3 rating says nothing about an audience that skews older . 11

7 Impact Analysis 11

8 The Complete Chain 12

9 Data Protection: Article by Article 12

10 Consumer Protection & Platform Disclosures 12

11 Regulatory & Legal Landscape 13

12 Indicators of Compromise & Reproducible Evidence 13

13 Disclosure Timeline & Outcome 14

14 What Oticon Got Right 14

15 Residual Risk & Recommendations 15

## Executive Summary

Oticon Companion is the Bluetooth companion app for Oticon hearing aids, built on the shared OneApp platform of Demant A/S. It has more than 1 million installs, Google Play lists it as a medical device, and the EU manufacturer of record is SBO Hearing A/S in Smørum. On 22 August 2026 RFI-IRFOS disclosed five findings from a root level code analysis of version 1.8.0 under REF OTICON-2026-R1.

This is one of the more carefully built apps in the programme. Cleartext traffic is denied and the production API host is pinned to a valid Sectigo certificate through 2036. Firebase collection is off at two independent layers. Local storage uses SQLCipher. Twelve separate consent definitions exist, and sensitive data logging is off by default. No advertising SDK and no PRC SDK was found. The findings sit beside that design.

One finding carries the weight. The app itself calls hearing aid information sensitive personal data related to hearing health, in the email support flow. The switch that gates HearingFitness wearing time tracking, the feature that collects the most hearing related data, offers to collect anonymous data to improve the app (H1). A production authorization key for api.demant.com is stored in plain text (M1), and two permissions with no visible purpose are declared (M3). The people behind the findings are users with hearing loss who decide on a consent switch whose wording understates what it collects.

The notice of 22 August 2026 went to three Oticon support addresses with the Austrian DSB and the EDPS in copy. The support system sent an automatic acknowledgement within thirty seconds. Follow-ups of 17 October and 15 November 2026 repeated the open points. No substantive reply is on record as of 21 November 2026. This report is published after the embargo date of 20 November 2026 was reached.

**Scope:** Root level code analysis of version 1.8.0 (versionCode 617548) of a .NET MAUI application: manifest, resources, configuration files, the native assembly store with its UI strings in 24 languages, and the four dex files of the Java interop layer. The binary came from an APKMirror bundle whose own manifest carries the Google Play distribution stamp, so the file was originally served through Google Play. The live Google Play listing was read on 2026-08-22. No device was used, no account was created, no traffic was intercepted and no Demant server was called. Items the package cannot show are marked UNVERIFIED.

| ID | Severity | Title |
|---|---|---|
| H1 | HIGH | Hearing aid data is called sensitive personal data related to hearing health in the support flow, and the consent switch that gates wearing time tracking calls it anonymous data |
| M1 | MEDIUM | An authorization key for the production backend api.demant.com is stored in plain text in the app configuration |
| M2 | MEDIUM | Firebase and Maps keys of the shared OneApp project oneapp-prod-13d7a are stored in plain text |
| M3 | MEDIUM | PACKAGE_USAGE_STATS and READ_PHONE_STATE are declared and the package shows no feature that uses them |
| L1 | LOW | No age verification is visible in the package, registration runs in a hosted flow, and the PEGI 3 rating says nothing about an audience that skews older |

### Finding Status at a Glance

| ID | Disclosed | This report | Status on 21 November 2026 |
|---|---|---|---|
| H1 | HIGH | HIGH | Open. Automatic acknowledgement only. |
| M1 | MEDIUM | MEDIUM | Open. Named in the notice. Automatic acknowledgement only. |
| M2 | MEDIUM | MEDIUM | Open. Not named in the notice text. |
| M3 | MEDIUM | MEDIUM | Open. Named in the notice. Automatic acknowledgement only. |
| L1 | LOW | LOW | Open. Not named in the notice text. |

## Subject & Operator Analysis

Google Play names Oticon A/S, Kongebakken 9, 2765 Smørum, Denmark, as developer, with the telephone number +45 39 17 73 00. The Play panel on EU medical device information names SBO Hearing A/S (SRN DK-MF-000001270) at the same address as manufacturer of record. Oticon is a brand of Demant A/S. The binary confirms the group: 114 of its 415 assemblies carry the prefixes Demant.MpHal, Demant.MpConfig or Demant.OneApp, the universal link domain is link.account.demant.com, the production API host is api.demant.com, and legacy assemblies carry the WDH prefix of the former William Demant Holding. The app configuration names itself AppInfo_ApplicationType OneApp and AppInfo_Brand Oticon, so the app is a branded build of one shared codebase. The same platform plausibly serves other Demant brands such as Philips HearLink, which is a reason to read the findings as structural.

The consent text in the app names Demant Enterprise A/S as the entity that processes the data in the support flow. The exact controller for the HearingFitness data is not stated in the package and is UNVERIFIED. With Danish establishments, the Danish Datatilsynet is the likely lead authority. The Österreichische Datenschutzbehörde is in copy of the notice. No data protection officer and no privacy policy URL was identified in the listing or the package, both are UNVERIFIED.

## Architecture & Data Flow

The application logic ships as 415 ahead-of-time compiled native libraries, one per .NET assembly, and a 33.7 MB assembly store that holds the managed metadata and all localized strings. Four dex files hold only the Java interop layer for AndroidX, Google Play Services, Firebase and ML Kit. The install bundle has 35 splits and 282 MB.

Sign-in uses the Microsoft Authentication Library with a hosted Entra ID or Azure AD B2C flow. The app talks to api.demant.com with a pinned certificate, to Firebase project oneapp-prod-13d7a, and to a video provider for teleaudiology. Consent is organised as twelve versioned definitions with their own identifiers, from anonymous data through battery and wax filter notifications to remote fitting. A data location feature lets users move their data, with a stated transfer time of up to 5 days. The runtime behaviour of that feature was not tested.

## Engagement Summary

The notice REF OTICON-2026-R1 was sent on 22 August 2026 at 12:02 UTC to contact-us@oticon.com, appsupport@oticon.com and appsupportus@oticon.com, with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It stated H1 in full, named the authorization key (M1) and the two permissions (M3) as medium findings, and asked for a written reply within 30 days. The support system of appsupport@oticon.com answered automatically at 12:02:48 UTC with a ticket number and the promise of an answer in less than 2 working days.

A follow-up from security@rfi-irfos.com went to the same three addresses on 17 October 2026 at 18:45 UTC, 34 days before the embargo date. A final notice titled 5 days to publication followed on 15 November 2026 at 13:01 UTC from s.kepp@rfi-irfos.com. No message from a person at Oticon or Demant is on record.

## Findings

### H1: Hearing aid data is called sensitive personal data related to hearing health in the support flow, and the consent switch that gates wearing time tracking calls it anonymous data

**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 assembly store of the app contains a company-written sentence that classifies hearing aid information as sensitive personal data related to hearing health. It appears once and applies only to the email support flow. The consent switch that gates the continuously running HearingFitness feature, which records how many hours per day the user wears the hearing aids, reads: Let us collect anonymous data to improve the app and user experience. In the consent registry of the app this switch is technically labelled AnonymousData. The registry has twelve entries and none of them carries a health data or special category label. The Play listing shows the app as a medical device, and its Data Safety section lists Health info among the collected data types. Wearing time of a prescribed hearing aid reveals a diagnosed condition and how consistently the treatment is followed. Data of that kind is data concerning health under Art. 9(1) and needs an Art. 9(2) exemption, in practice explicit consent that names the category. RFI-IRFOS blast-radius escalation: raised from none to HIGH because the data belongs to a special category, the app is rated as a medical device with more than 1 million installs, and the operator's own text shows that it knows the category is sensitive. The CVSS vector scores zero because this is a consent wording finding with no technical attack path.

```
By contacting the email support, I agree that Demant Enterprise A/S may process my
    personal
data disclosed in this email, including the attachments, to handle my request. I am
    aware
that this email and the attachment may contain sensitive personal data related to
    hearing
health (hearing aid information). This data may be used to answer my request and
    improve
the app.
```

```
ConsentDefinitionId_AnonymousData = 0B01C85D-3A5F-4F93-AD56-EA3B64E5D8B3   (assets/app
    .config)

ToggleConsent_AnonymousDataUsageContent:
  Let us collect anonymous data to improve the app and user experience.

HearingFitness lets you check how long you wear hearing aids every day and track your
    progress.
Hearing aids track your wearing time. When you connect them to the app, we link
    wearing time
to a specific day.
```

**Impact:** A person with hearing loss who switches on wearing time tracking reads that anonymous data is collected. The same app calls this kind of data sensitive health information when the person writes to support. The consent the person gave was shaped by the first wording.

**Fix:** Rename and re-word the consent for HearingFitness so that it names health data and hearing aid wearing time, record it as an explicit Art. 9(2)(a) consent, and carry the wording used in the support flow over to every screen that gates the same category.

### M1: An authorization key for the production backend api.demant.com is stored in plain text in the app configuration

---

**MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), disclosed as MEDIUM, open**

The file assets/app.config holds a base64 value named Ccs_AuthorizationKey together with the endpoint https://api.demant.com/ccs/v1. The file ships unencrypted in every installed copy and can be read with unzip. Google documents that Firebase keys are safe to ship in a client (see M2). Demant has published no equivalent statement for this key, and its name describes a credential rather than a public identifier. Whether it only identifies the app version or grants API access of its own cannot be seen from the package. No call was made against api.demant.com. The burden of showing that an extracted key cannot be reused for calls outside the app sits with the controller under Art. 32(1)(b) and Art. 25.

```
<add key="Ccs_AuthorizationKey" value="X2QjUYKIvMcV8BEpajncJNai0cUtseBHoKj2W/
    IUd0b8lQziu/O13g==" />
<add key="Ccs_Endpoint" value="https://api.demant.com/ccs/v1" />
<add key="Ccs_Environment" value="" />
<add key="Ccs_Module" value="mobile" />
<add key="Ccs_System" value="android" />
```

**Impact:** Anyone can copy the key from an installed app. If the backend relies on it as a credential, a third party could send requests that look like they come from the app, with the load or data exposure that follows.

**Fix:** State what the key authorizes. Rotate it if it is meant to be a credential, and make every call depend on per-user authentication on the server.

### M2: Firebase and Maps keys of the shared OneApp project oneapp-prod-13d7a are stored in plain text

**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 MEDIUM in the findings file, not named in the notice text, open**

Firebase values sit in res/values/strings.xml and a Google Maps key sits in the manifest. A Firebase key is not secret by Google design, so this is not a confidentiality finding. It is recorded because the project name oneapp-prod-13d7a confirms that the Firebase project is the shared project of the OneApp platform, and because Crashlytics, Storage and Common bindings are present although collection is off by default. Whether the Maps key is restricted by package and certificate was not tested.

```
<string name="google_api_key">AIzaSyAeHYev5ZdyNb8UrinLQG70kvMXLsJO2Ms</string>
<string name="google_app_id">1:840039602875:android:f776e101a5b12a1a5b279e</string>
<string name="google_storage_bucket">oneapp-prod-13d7a.appspot.com</string>
<string name="project_id">oneapp-prod-13d7a</string>
<string name="gcm_defaultSenderId">840039602875</string>

<meta-data android:name="com.google.android.geo.API_KEY" android:value="
    AIzaSyDxXATqDTYxi_VsUNHjDXlsH0Q_undtelg"/>
```

**Impact:** The keys give nobody access to user data by themselves. An unrestricted Maps key could be used by others and billed to the operator.

**Fix:** Restrict the Maps key by package name and signing certificate and confirm that the Firebase rules of oneapp-prod-13d7a deny unauthenticated access.

### M3: PACKAGE_USAGE_STATS and READ_PHONE_STATE are declared and the package shows no feature that uses them

**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 MEDIUM, open**

PACKAGE_USAGE_STATS is a special access permission that lets an app see which other apps the user runs and for how long. The user must grant it by hand in the Usage Access settings. READ_PHONE_STATE gives access to device identifiers and call state. A search of about 50,000 UTF-16 resource names and about 112,000 UTF-8 resource values in the assembly store found no reference to UsageStatsManager, queryUsageStats, TelephonyManager, PhoneStateListener or getCallState. Every other sensitive permission in the manifest has an identifiable feature behind it. The permissions may be left over from a shared library. The package does not confirm that, and active use behind a code path that is not visible in the strings cannot be excluded.

```
<uses-permission android:name="android.permission.PACKAGE_USAGE_STATS"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
```

**Impact:** If the permissions are in use, a person who treats a hearing condition shares a record of their app usage and phone state with a hearing aid app. If they are unused, the app asks for more than it needs.

**Fix:** Remove both permissions or document the feature that needs them.

### L1: No age verification is visible in the package, registration runs in a hosted flow, and the PEGI 3 rating says nothing about an audience that skews older

**LOW, 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 LOW, open**

No date of birth field, age gate, legal age statement or parental consent string appears in res/values/strings.xml or in the strings of the assembly store, which holds the UI text in 24 languages. Account creation and sign-in run through the Microsoft Authentication Library against a Microsoft Entra ID or Azure AD B2C tenant, so the registration form is rendered by a hosted page outside the package. The absence of an age gate in the package is therefore inconclusive. If an age check exists it lives in the hosted flow, which this analysis did not open. The Play listing shows PEGI 3. That is accurate for content, and the real audience of a hearing aid app skews towards older adults, for whom the consent design under H1 matters more than any age rating. No Art. 8 finding is made.

```
<activity android:name="crc64ed1888fb4925e3b7.AuthenticationAgentActivity" android:
    theme="@style/MsalTheme" .../>
<activity android:exported="true" android:name="crc648316b0a9aa8cfd61.
    BrowserTabActivity">
  <intent-filter><data android:host="auth" android:scheme="msaloneappoticon"/></intent
    -filter>
</activity>

FeatureToggle_IsAccountCreationEnabled=True   (assets/app.config)
```

**Impact:** The finding is an observation about the audience. It does not describe a harm that was shown.

**Fix:** Publish the age handling of the hosted registration flow and keep consent wording legible for older users.

## Impact Analysis

The people affected are users of an app with more than 1 million installs who wear hearing aids. The data concerns hearing health: wearing time per day, device serial, connected hearing aids, remote fitting sessions and account data. A large share of the audience is older.

H1 affects every user who decides on the HearingFitness switch. M1 and M2 concern backend and platform credentials. M3 concerns two permissions that the package does not explain. L1 concerns the registration flow and audience fit.

The demonstrated harm is a harm of consent quality. No access to user data was shown and none was attempted.

## The Complete Chain

Step 1, install: the person installs a medical device companion app.

Step 2, sign-in: a hosted flow creates the account. The age handling is not visible (L1).

Step 3, consent: the HearingFitness switch asks to collect anonymous data to improve the app. The registry labels it AnonymousData (H1).

Step 4, use: wearing time is linked to a specific day and device. Requests go to api.demant.com under an embedded key (M1). Two unexplained permissions are declared (M3).

Step 5, support: if the person writes to support, the app now calls the same kind of information sensitive personal data related to hearing health (H1).

## Data Protection: Article by Article

Article 9(1) and 9(2), special categories: engaged by H1.

Article 6(1) and Article 7(1), lawfulness and conditions for consent: engaged by H1.

Article 5(1)(a), lawfulness, fairness and transparency: engaged by H1 and L1.

Article 13(1)(c), purposes and legal basis: engaged by H1.

Article 5(1)(c), data minimisation: engaged by M3.

Article 25, data protection by design and by default: engaged by M1, M2 and M3.

Article 32(1)(b), security of processing: engaged by M1 and M2.

## Consumer Protection & Platform Disclosures

The Google Play listing shows the app as Oticon Companion by Oticon A/S, updated on 24 June 2026, with 1 million or more installs, about 18,800 reviews, a rating of 3.7 and the label Medical device. The Data Safety section lists Health info among the collected data types. The listing carries a PEGI 3 rating. The listing was read on 2026-08-22.

## Regulatory & Legal Landscape

The framework applied is the GDPR, with Article 9 for data concerning health. The operator is established in Denmark, so the Danish Datatilsynet is the likely lead authority under Article 56. The Österreichische Datenschutzbehörde (dsb@dsb.gv.at) and the European Data Protection Supervisor (edps@edps.europa.eu) are in copy of the notice 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.oticon.app
Version            1.8.0 (versionCode 617548), analysed 2026-08-22
base.apk SHA-256   acc8f305dab947806e997c989c6759e00b2d6bbf49589fe1efe43a69b722c767
APKM bundle SHA-256 2841c293e1bb693d86bf6a5ab9ad290996c4122d34eba29d4c7acad99c26a304
minSdk / targetSdk 26 / 36

ConsentDefinitionId_AnonymousData 0B01C85D-3A5F-4F93-AD56-EA3B64E5D8B3
Ccs_AuthorizationKey X2QjUYKIvMcV8BEpajncJNai0cUtseBHoKj2W/IUd0b8lQziu/O13g==
Ccs_Endpoint         https://api.demant.com/ccs/v1

Firebase project   oneapp-prod-13d7a
google_api_key     AIzaSyAeHYev5ZdyNb8UrinLQG70kvMXLsJO2Ms
google_app_id      1:840039602875:android:f776e101a5b12a1a5b279e
Storage bucket     oneapp-prod-13d7a.appspot.com
sender id          840039602875
Maps key           AIzaSyDxXATqDTYxi_VsUNHjDXlsH0Q_undtelg
```

```
H1  lib/arm64-v8a/libassembly-store.so (support consent text, HearingFitness texts),
    assets/app.config (ConsentDefinitionId_*)
M1  assets/app.config (Ccs_*)
M2  res/values/strings.xml, AndroidManifest.xml (com.google.android.geo.API_KEY)
M3  AndroidManifest.xml (PACKAGE_USAGE_STATS, READ_PHONE_STATE), assembly store string
     search
L1  AndroidManifest.xml (MSAL activities), assets/app.config (
    FeatureToggle_IsAccountCreationEnabled)
```

Reproduction: obtain com.oticon.app 1.8.0 from Google Play or the APKMirror bundle above, check the SHA-256, unzip the base and the arm64 split, decode the manifest and read the named files. The string checks for M3 use a UTF-16 and UTF-8 string extraction of the assembly store. No device, account or network access is needed.

## Disclosure Timeline & Outcome

2026-08-22 12:02 UTC Notice REF OTICON-2026-R1 to contact-us@oticon.com, appsupport@oticon.com and appsupportus@oticon.com, CC DSB and EDPS. Finding H1 in full, M1 and M3 named, reply window 30 days.

2026-08-22 12:02 UTC Automatic acknowledgement from appsupport@oticon.com with a ticket number.

2026-10-17 18:45 UTC Follow-up from security@rfi-irfos.com to the same addresses, 34 days before the embargo date.

2026-11-15 13:01 UTC Final notice from s.kepp@rfi-irfos.com, titled 5 days to publication, naming 20 November 2026 as the embargo date.

2026-11-20 Embargo date, 90 days after delivery of the notice of 22 August 2026. No substantive reply has been received as of 21 November 2026.

## What Oticon Got Right

The base configuration denies cleartext traffic, and the production API host api.demant.com is pinned to a Sectigo certificate that is valid through 21 March 2036 and applies to subdomains. Firebase Analytics, Crashlytics, Performance and advertising ID collection are off in the manifest, and the runtime default Firebase_UploadCrashLogs is False. The local database uses SQLCipher. The consent registry holds twelve versioned definitions with separate identifiers, and the remote assistance feature has its own consent screen with a disagree button and a withdrawal path. Logging of sensitive data is off by default (Log_EnableLoggingSensitiveData False, minimum level Error). A persistent machine ID is off (FeatureToggle_CreatePersistentMachineId False). No advertising mediation SDK and no PRC SDK was found. BLUETOOTH_SCAN carries neverForLocation, allowBackup is false, and sign-in uses Microsoft Entra ID instead of a home made identity system. A user facing data location feature exists.

## Residual Risk & Recommendations

Open at the date of publication: all five items, with no written position from the operator. Items that only the operator can close are the consent wording and legal basis behind HearingFitness (H1), the scope of the Ccs key (M1), the reason for the two permissions (M3) and the age handling of the hosted registration (L1).

Recommendations: carry the sensitive data wording from the support flow into every consent screen that gates the same category, record an explicit Art. 9(2)(a) consent, state and limit what the Ccs key authorizes, restrict the Maps key, and remove or explain PACKAGE_USAGE_STATS and READ_PHONE_STATE.

This report is published after the embargo date. Statements are limited to the package and to the public documents named above, and every item the package cannot show is marked UNVERIFIED.

**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 and public documents. No servers or accounts probed. Final report, published 21 November 2026. REF OTICON-2026-R1.