Security & Privacy Disclosure, Final Report

Philips Sonicare for Android (com.philips.cdp.ohc.tuscany)

A toothbrush app whose store label says nothing is shared, while its own privacy notice names seven recipients and sends rights requests to a Chinese domain.

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

Target	Philips Oral Healthcare, LLC, Bothell, Washington, USA (controller named in the app)
Versions Audited	10.20.0 / 254 (2026-08-22)
Notice / Publication	2026-08-22 / 2026-11-20 (90 days)
Findings	9: 3 High, 4 Medium, 1 Low, 1 observation
Status	No reply of any kind as of 21 November 2026, not even an automatic acknowledgement, to the notice or to the two follow-ups.
SHA-256 (base APK)	`c9ae8c8077d1dc1f2c11443f80a3ace658465c9afc3d1c2251b99c519a072375`

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 5

3 Subject & Operator Analysis 5

4 Architecture & Data Flow 6

5 Engagement Summary 6

6 Findings 7

6.1 C1: The Google Play Data Safety label says no data is shared with third parties, while the privacy notice and consent text inside the same app name seven recipients . . . 7

6.2 H1: FirebaseInitProvider starts at the highest priority in the manifest and no override disables Firebase Analytics collection . . . 9

6.3 H2: Only a Union-external controller is named for every market outside China, no Article 27 representative appears, and the only contact link points to a Chinese-market domain . . . 10

6.4 H3: A Sonicare For Kids handle is listed as a supported product in the adult app, with no age control stronger than a self-reported question . . . 11

6.5 M1: Advertising identifier and Privacy Sandbox attribution are open to all partners in an app that shows no ads . . . 12

6.6 M2: Firebase, Amazon, product registration, e-commerce and per-country identity credentials are shipped in plain text . . . 13

6.7 M3: READ_CALENDAR is requested although the stated purpose, creating reminders, needs only write access . . . 14

6.8 L1: No technical age verification, only a self-reported age range and a free text date of birth . . . 14

6.9 L2: WeChat, ICP and China-specific identity infrastructure in the global binary, confirmed gated to Greater China . . . 15

7 Impact Analysis 15

8 The Complete Chain 16

9 Data Protection: Article by Article 16

10 Consumer Protection & Platform Disclosures 17

11 Regulatory & Legal Landscape 17

12 Indicators of Compromise & Reproducible Evidence 18

13 Disclosure Timeline & Outcome 19

14 What Philips Got Right 19

15 Residual Risk & Recommendations 19

Executive Summary

Philips Sonicare is the Bluetooth companion app for connected Sonicare toothbrushes. Google Play lists Philips Consumer Lifestyle B.V. as developer, with more than 1 million installs and a PEGI 3 rating. The privacy notice inside the app names a different entity, Philips Oral Healthcare, LLC of Bothell, Washington, as controller. On 22 August 2026 RFI-IRFOS disclosed nine findings from a root level code analysis of version 10.20.0 under REF SONICARE-2026-R1.

The engineering is careful in several places. Cleartext traffic is denied everywhere, backup and device transfer are excluded for every data category, BLUETOOTH_SCAN carries neverForLocation, no camera or microphone permission is requested, account deletion works from inside the app, and a regional consent table keeps WeChat functionality away from users in the Union. The findings sit beside that design.

Three findings carry the weight. The Data Safety label says no data is shared with third parties, and the privacy notice and consent text in the same package name Amazon, Adobe, Apptentive, Branch Metrics, Delta Dental and Henry Schein (C1). Firebase starts at the highest provider priority in the manifest with no Analytics override (H1). The only rights contact for every market outside China is a page on a Chinese domain, and no Union representative is named (H2). The people behind the findings are users who brush with a connected toothbrush and cannot reach the controller of their data.

The notice of 22 August 2026 went to OHCAppSupport@philips.com and privacy@philips.com with the Austrian DSB and the EDPS in copy. Follow-ups of 17 October 2026 and 15 November 2026 repeated the three questions and the embargo date of 20 November 2026. No reply of any kind, not even an automatic one, is on record 91 days after delivery, and no delivery failure was returned. The embargo date has passed and this report is published on 21 November 2026.

Scope: Root level code analysis of the Google Play release 10.20.0 (versionCode 254): manifest, resources, bundled assets and dex string pool. The live Google Play listing and Data Safety section were read on 2026-08-22. No Philips server, database or bucket was called, no account was created, no traffic was intercepted and no runtime instrumentation was used. The native libraries in the arm64 split were not analysed. Items the package cannot show are marked UNVERIFIED.

ID	Severity	Title
C1	HIGH	The Google Play Data Safety label says no data is shared with third parties, while the privacy notice and consent text inside the same app name seven recipients
H1	HIGH	FirebaseInitProvider starts at the highest priority in the manifest and no override disables Firebase Analytics collection
H2	HIGH	Only a Union-external controller is named for every market outside China, no Article 27 representative appears, and the only contact link points to a Chinese-market domain
H3	MEDIUM	A Sonicare For Kids handle is listed as a supported product in the adult app, with no age control stronger than a self-reported question
M1	MEDIUM	Advertising identifier and Privacy Sandbox attribution are open to all partners in an app that shows no ads
M2	MEDIUM	Firebase, Amazon, product registration, e-commerce and per-country identity credentials are shipped in plain text
M3	MEDIUM	READ_CALENDAR is requested although the stated purpose, creating reminders, needs only write access
L1	LOW	No technical age verification, only a self-reported age range and a free text date of birth
L2	INFO	WeChat, ICP and China-specific identity infrastructure in the global binary, confirmed gated to Greater China

ID	Disclosed	This report	Status on 21 November 2026

Finding Status at a Glance

ID	Disclosed	This report	Status on 21 November 2026
C1	CRITICAL	HIGH	Open. No reply of any kind.
H1	HIGH	HIGH	Open. No reply of any kind.
H2	HIGH	HIGH	Open. No reply of any kind.
H3	HIGH	MEDIUM	Open. No reply of any kind.
M1	MEDIUM	MEDIUM	Open. Summarised in the notice, no reply.
M2	MEDIUM	MEDIUM	Open. Summarised in the notice, no reply.
M3	MEDIUM	MEDIUM	Open. Summarised in the notice, no reply.
L1	LOW	LOW	Open. Not in the notice text.
L2	LOW or informational	INFO	Observation. Not in the notice text.

Subject & Operator Analysis

The Privacy Notice bundled in the app names Philips Oral Healthcare, LLC, 22100 Bothell Everett Highway, Bothell WA 98021, USA, as controller for every market outside Mainland China. For Mainland China it names Philips (China) Investment Co., Ltd., Building A1, No. 718 Lingshi Road, Jing'an District, Shanghai, as the entrusted entity. Google Play names Philips Consumer Lifestyle B.V., High Tech Campus 34, 5656 AE Eindhoven, Netherlands, as developer, with the contact noreply.app@philips.com. The two entities differ, and the app does not explain how they relate.

No Union establishment or Article 27 representative is named for the controller. For an Austrian initiated matter the Österreichische Datenschutzbehörde is the first contact. The one-stop-shop mechanism does not apply in the usual way without a confirmed main establishment in the Union, which is part of H2. The mailbox privacy@philips.com is the group level privacy contact on the public record and was not verified as the data protection officer of this controller.

The identity layer of the app uses a Philips Identity Management resource named philipsmobileappsauroraprod and endpoints on philips-healthsuite.com. Both belong to Philips wide infrastructure and are not specific to Sonicare. The Firebase project ph-ohc-sonicare is dedicated to this app.

Architecture & Data Flow

The app is a native Android application with six dex files of about 41.7 MB. An embedded PyTorch ExecuTorch test runner and Google ML Kit barcode scanning suggest on-device inference for brush motion and barcode features. The package does not confirm it. The tier names Essential, Advanced and Premium on the Play listing follow the physical handle detected over Bluetooth. No billing SDK, no RevenueCat, no Stripe and no paywall exists in the package. The only subscription in the code is Amazon's physical brush head replenishment service.

The app talks to Firebase, Adobe Analytics, Apptentive, Branch Metrics, Amazon Login with Amazon and the Philips identity and health cloud hosts. Consent handling uses a region table in assets/PrivacyNotice.json with the buckets analytics, tcp and tencent. Austria sits in the analytics opt-in bucket. Firebase starts from a content provider before any screen (H1).

Engagement Summary

The notice REF SONICARE-2026-R1 was sent on 22 August 2026 at 12:04 UTC to OHCAppSupport@philips.com and privacy@philips.com, with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It stated C1, H1, H2 and H3 with verbatim evidence, summarised the medium and low findings, credited the design, asked three questions and quoted Article 33(4) GDPR on the notification clock.

A follow-up with the same three questions went from security@rfi-irfos.com to the same two addresses on 17 October 2026 at 18:51 UTC, 34 days before the embargo date. No message from Philips or from a representative is on record, and no automatic acknowledgement arrived. A further follow-up from security@rfi-irfos.com on 15 November 2026 at 12:56 UTC, five days before the embargo date, repeated the open findings and the three questions. No answer arrived, and all three questions remain open as of 21 November 2026.

Findings

C1: The Google Play Data Safety label says no data is shared with third parties, while the privacy notice and consent text inside the same app name seven recipients

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

The Data Safety section of the app, read live on 2026-08-22, states: No data shared with third parties. The Privacy Notice bundled in the package as assets/html/privacy_policy_summary.html states: We share the following data with Amazon, the generic model ID of your Device and when your brush head is at a high (80%) or low (20%) wear range. It also lists a section titled Enabling you to share your data with third parties, naming Insurance or oral healthcare providers and Apple Health. The onboarding consent text NEW_ONBG_ANALYTICS_NOTICE names Adobe Analytics, Apptentive, Branch Metrics and Google Firebase Crashlytics, and says Branch collects the Android Advertiser ID and the Apple IDFA. Two further consent strings name Delta Dental and Henry Schein. The SDK classes and endpoints of these recipients are present in the dex files. Rating basis: the contradiction between two documents of the same package is verified. Google defines sharing for the Data Safety section so that transfers to service providers acting for the developer and transfers the user starts themselves are not counted, which may cover part of the list. The Amazon reorder data, the advertising identifier collected by Branch and the insurance route are described in the notice itself as sharing. RFI-IRFOS blast-radius escalation: raised from none to HIGH because the app has more than 1 million installs, the Data Safety section is the statement users rely on before installing, and the operator's own bundled documents contradict it in the operator's own words. The CVSS vector scores zero because this is a transparency finding with no technical attack path.

```
The live Data Safety section (fetched 2026-08-22):
  This app may collect these data types: Personal info, Health and fitness and 4
    others
  Data is encrypted in transit
  No data shared with third parties

assets/html/privacy_policy_summary.html:
  Smart Reorder Service. We share the following data with Amazon: the generic model ID
     of
  your Device and when your brush head is at a 'high' (80%) or 'low' (20%) wear range
    ("Smart Reorder Data").
  Enabling you to share your data with third parties.
  - Insurance or oral healthcare providers.
  - Apple Health.
```

```
<string name="DART_EXP_SET_REORDER_CONSENT">I consent to share my toothbrush and
    account information with Amazon.</string>
<string name="DELTA_DENTAL_CONSENT_TEXT">I allow Philips Sonicare to share my brushing
     data with Delta Dental to receive Sonicare approved insurance benefits.</string>
<string name="HENRY_SCHEIN_CONSENT_TEXT">I allow my brushing data to be shared with
    Henry Schein.</string>

NEW_ONBG_ANALYTICS_NOTICE names: Adobe Analytics (Adobe Systems Software Ireland
    Limited), Apptentive (Apptentive Inc.),
Branch Metrics (Branch Metrics, Inc., "Android Advertiser ID, GAID" and Apple "IDFA"),
     Google Firebase Crashlytics.

Dex evidence: com.adobe.assurance, apptentive.com.android.feedback.
    ApptentiveDefaultClient, DartAmazonBanner,
hosts api.apptentive.com, assets.adobedtm.com, app-measurement.com, www.deltadentalins
    .com
```

Impact: A person who reads the Data Safety section before installing a toothbrush app is told that nothing is shared with third parties. The same app then shows its own text naming insurers, a dental supplier, an online retailer and an attribution company. The person decided on the first statement and is bound by the second.

Fix: Correct the Data Safety section so that it matches the Privacy Notice and the consent text, or explain in writing which named recipients are service providers or user initiated transfers and publish that classification.

H1: FirebaseInitProvider starts at the highest priority in the manifest and no override disables Firebase Analytics collection

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

FirebaseInitProvider is declared with initOrder 100, directBootAware true, which is the highest initialisation priority in the manifest. The next highest is MlKitInitProvider at 99. Content providers run at process start, before any Activity, so before any consent screen can render. The manifest sets firebase_crashlytics_collection_enabled, firebase_performance_collection_enabled and google_analytics_adid_collection_enabled to false, and no firebase_analytics_collection_enabled flag exists anywhere in the package. Without that override the Firebase default is to start Analytics collection once the provider has run. The package holds a consent notice and a regional consent table, so an application level call may switch collection off before any event is sent. That code path was not traced, and no traffic was captured. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the app is rated PEGI 3, has more than 1 million installs and also lists a children's brush (H3), and the provider runs before any consent can be shown. The CVSS vector scores only the technical exposure of low-sensitivity telemetry.

```
<provider android:authorities="com.philips.cdp.ohc.tuscany.firebaseinitprovider"
          android:directBootAware="true" android:exported="false"
          android:initOrder="100"
          android:name="com.google.firebase.provider.FirebaseInitProvider"/>

$ grep -rn "firebase_analytics_collection_enabled" sc_dec/
(no match)
```

Impact: On the default Firebase configuration, usage events of a brushing app start with the process, before the person has seen or answered any consent text.

Fix: Set firebase_analytics_collection_enabled to false in the manifest and enable collection in code only after a recorded consent decision.

H2: Only a Union-external controller is named for every market outside China, no Article 27 representative appears, and the only contact link points to a Chinese-market domain

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 Privacy Notice bundled in the package is the only English language variant, the only other locale directory is assets/html/zh. It names Philips Oral Healthcare, LLC, Bothell, Washington, USA as controller for every market outside Mainland China. No Union establishment and no Article 27 representative is named anywhere in the package. The single link offered for questions about the notice and for exercising rights is https://www.philips.com.cn/c-e/privacy-request.html, in the same document shown to users in Austria. The Google Play developer of record is a different entity, Philips Consumer Lifestyle B.V. in Eindhoven, whose only listed contact is a no-reply address. The heading Wo we are is quoted as shipped. Whether the Chinese link works for a request from the Union was not tested. RFI-IRFOS blast-radius escalation: raised from none to HIGH because the only rights path the app offers to users outside China leads to a Chinese-market page, for an app with more than 1 million installs. The CVSS vector scores zero because this is a legal and transparency finding with no technical attack path.

```
<p><b>Wo we are?</b></p>
<p>The data controller of your data is Philips Oral Healthcare, LLC with address at
22100 Bothell Everett Highway, Bothell WA 98021, USA. However, if you are subject to
    the privacy
and data protection laws and regulations of Mainland China, we, Philips (China)
    Investment Co., Ltd.
... located at Building A1, No. 718 Lingshi Road, Jing'an District, Shanghai, as the
    entity entrusted
by Philips Oral Healthcare, LLC, responsible for collecting, processing personal
    information and
handling privacy and data protection related matters within Mainland China.</p>

<p><b>Contact Us</b></p>
<p>If you have any questions about this Privacy Statement...you can click
<a href="https://www.philips.com.cn/c-e/privacy-request.html">here</a> to contact
    Philips.</p>
```

Impact: A user in Austria who wants to see or delete the brushing data held about them is sent to a page on a Chinese domain, written for another legal regime, and told that a US company is the controller. Nobody in the Union is named as a contact.

Fix: Name a Union representative or establishment in the app and in the notice, and give every market outside China a working rights request channel that is not a Chinese-market page.

H3: A Sonicare For Kids handle is listed as a supported product in the adult app, with no age control stronger than a self-reported question

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, rated MEDIUM in this report, rated MEDIUM by blast-radius escalation

The per-market file assets/ProductsConfiguration_AT.json lists the model HX6322/04 under SonicareForKids, inside a block named ShopForProducts. Nine of the 57 market files were sampled (AT, DE, US, GB, FR, NL, CN, RU, JP) and all carry the same entry. The resource table has a product type label Sonicare For Kids. No parental, COPPA, under 13, under 16 or under 18 string exists. The only age mechanisms are a self-reported onboarding question, My age range is, and a free text Date of birth field in the account profile. A separate Philips Sonicare For Kids app exists on Google Play. Rating basis: the package shows the product entry and the label, but the block name points to a shop list and the pairing flow for this handle was not shown. A parent managing a child's brushing under the parent's own account is a common and legitimate pattern that this report does not object to. RFI-IRFOS blast-radius escalation: raised from none to MEDIUM because a child may be the person behind the data, and the package contains no control that separates a child's data from an adult's. The CVSS vector scores zero because this is a legal and design finding with no technical attack path.

```
// assets/ProductsConfiguration_AT.json, block "ShopForProducts"
"SonicareForKids": [
    "HX6322/04"
]

<string name="PROD_TYPE_SONICARE_KIDS">Sonicare For Kids</string>
<string name="age">4. My age range is:</string>
<string name="mya_Date_of_birth">Date of birth</string>
```

Impact: If a child's brush is connected, the child's brushing data would run through the same Firebase project and the same attribution and analytics pipeline as an adult's. The package contains nothing that would route a minor's data differently.

Fix: State whether a Kids handle can be paired in this app. If it can, add an age appropriate consent route that keeps children's data out of the attribution pipeline.

M1: Advertising identifier and Privacy Sandbox attribution are open to all partners in an app that shows no ads

MEDIUM, CVSS v4.0 AV:N/AC:L/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, open

The manifest requests AD_ID, ACCESS_ADSERVICES_ATTRIBUTION and ACCESS_ADSERVICES_AD_ID and ships an ad services configuration with allowAllToAccess set to true. The dex files contain no advertising display SDK, checked for AdMob, AppLovin, Unity Ads, ironSource and InMobi. The app has no billing SDK and no paid feature. The advertising identifier is used for attribution through Branch Metrics, which the app's own consent text states. The least restrictive setting grants every attribution partner access instead of a named list.

```
<uses-permission android:name="com.google.android.gms.permission.AD_ID"/>
<uses-permission android:name="android.permission.ACCESS_ADSERVICES_ATTRIBUTION"/>
<uses-permission android:name="android.permission.ACCESS_ADSERVICES_AD_ID"/>
<property android:name="android.adservices.AD_SERVICES_CONFIG" android:resource="@xml/
    ga_ad_services_config"/>

<!-- res/xml/ga_ad_services_config.xml -->
<ad-services-config>
    <attribution allowAllToAccess="true" />
</ad-services-config>
```

Impact: A person who bought a connected toothbrush gets a persistent cross-app identifier collected for marketing measurement, in an app that has no ads to fund. Buying the premium handle changes the coaching and does not change this.

Fix: Replace allowAllToAccess with a named partner list and tie the advertising identifier to a recorded consent.

M2: Firebase, Amazon, product registration, e-commerce and per-country identity credentials are shipped in plain text

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 Firebase key and project values sit in res/values/strings.xml. The file assets/api_key.txt is a bare file holding a signed Login with Amazon API key token, whose decoded payload is shown below. The file assets/AppConfig.json carries a Product Registration API key, an e-commerce API key and the Philips Identity Management client API keys for CN, RU and the default set, plus a WeChat app ID and a China ICP filing number. A Firebase key is not secret by Google design. The Amazon token and the identity keys are authentication material for account linking and identity federation, so they belong to a different class. Whether the server side scopes of these keys are narrow is not shown by the package and no call was made.

```
<string name="google_api_key">AIzaSyAKwcJy9SUiCDxtJjx9Q6Yu26-a2ou6Tio</string>
<string name="google_app_id">1:196989047715:android:788f3456b22f61c3418016</string>
<string name="project_id">ph-ohc-sonicare</string>
<string name="google_storage_bucket">ph-ohc-sonicare.appspot.com</string>
<string name="default_web_client_id">196989047715-rqm7f4enmiev8bgquh70mdn6gmid3hd1.
    apps.googleusercontent.com</string>
```

```
{
  "endpoints": {"authz": "https://www.amazon.com/ap/oa", "tokenExchange": "https://api
    .amazon.com/auth/o2/token"},
  "clientId": "amzn1.application-oa2-client.9421e1db14e341d5adfc3e7bb3ca8e86",
  "appFamilyId": "amzn1.application.a738afd4b80b4b3c9df765a5999e1448",
  "iss": "Amazon", "type": "APIKey", "pkg": "com.philips.cdp.ohc.tuscany",
  "appsigSha256": "D2:D6:95:A1:1D:1B:84:F9:25:A9:45:6E:27:F4:45:E9:FD:87:C3:74:63:AA:8
    A:34:32:A6:6A:23:3B:0F:D5:0F"
}
```

```
"ProductRegistration": {"ApiKey": "IQytAjOkX43QmYQ0R7MiG9vJzQX9evBJ2kZEPKgU"},
"MEC": {"PIL_ECommerce_API_KEY": "yaTmSAVqDR4GNwijaJie3aEa3ivy7czu22BxZwKP"},
"PIM": {
  "apiKey": "{\"CN\":\"IRZthgIyd72LE39zqoRsW5TZ6MMOnFEV9LDfFwRs\",\"RU\":\"
    ochuwzHTrQax4IQiWQn3m9JJab70ETP29L3xUAtY\",\"default\":\"
    xpbccXhsgr4J9h6eFzznq9JYz2Ag7sGl5awGL4Xq\"}",
  "weChatAppId": "wx53fa669d65050e61",
  "icpFilingNumber": □"□□ICP09062110-13A"
}
```

Impact: Anyone can read these keys from an installed copy. If the matching server side scopes are wide, a third party could attempt to impersonate the app against the Amazon and identity services that hold account links of people who brush with this app.

Fix: Move the credentials out of the package where possible, rotate the keys that are not meant to be public, restrict the rest by package and certificate, and publish the server side

scope of each.

M3: READ_CALENDAR is requested although the stated purpose, creating reminders, needs only write access

---

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

The manifest requests READ_CALENDAR. The dex files reference CalendarContract Calendars, Events and Reminders. The bundled Privacy Notice discloses the Calendar permission under its Permissions heading, so the capability is declared. READ_CALENDAR lets an app query titles, attendees, locations and times of every calendar on the device, while a reminder feature needs to insert entries. Whether the reminder code ever queries existing events was not traced.

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

$ grep -o "Landroid/provider/CalendarContract\$[A-Za-z]*;" classes*.dex
Landroid/provider/CalendarContract$Calendars;
Landroid/provider/CalendarContract$Events;
Landroid/provider/CalendarContract$Reminders;
```

Impact: A person who grants the permission for a brush head reminder also opens medical and personal appointments in the same calendar to the app.

Fix: Request only the write permission the reminder feature needs, or document why read access is required.

L1: No technical age verification, only a self-reported age range and a free text date of birth

---

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 validation, no eligibility gate and no minimum age Terms clause exists in the package. The only age related items are the self-reported onboarding question and the free text profile field shown under H3. This item stands on its own and is comparable to the age finding for other toothbrush apps in the programme, which also found self-declaration only.

```
<string name="age">4. My age range is:</string>
<string name="mya_Date_of_birth">Date of birth</string>
```

Impact: Nothing stops a minor from creating an account and entering any age.

Fix: Add a minimum age statement to the terms the user accepts and validate the date of birth field.

L2: WeChat, ICP and China-specific identity infrastructure in the global binary, confirmed gated to Greater China

INFO, no CVSS v4.0 score assigned, observation, disclosed as LOW or informational

The manifest registers two WeChat integration activities and queries the WeChat package. The dex files reference the WeChat Open SDK and api.weixin.qq.com. AppConfig.json carries a China ICP filing number and a China-specific identity backend at www.authz.accounts.philips.com.cn. The bundled PrivacyNotice.json gates the Tencent bucket to TW, MO, HK and CN, and places Austria in the analytics opt-in bucket with the rest of the EU and EEA. No evidence was found that this code activates for users in the Union. No Article 44 violation is asserted.

```
<queries><package android:name="com.tencent.mm"/></queries>
<activity android:exported="true" android:name="com.philips.cdp.ohc.tuscany.wxapi.
    WXEntryActivity" .../>

PrivacyNotice.json:  { "tencent": ["TW", "MO", "HK", "CN"] }
```

Impact: Recorded for transparency about the architecture. The regional gating in the package is a design that works in favour of users in the Union.

Fix: No action required. A short note in the Privacy Notice on the regional gating would help readers.

Impact Analysis

The people affected are users of a toothbrush app with more than 1 million installs. The data includes brushing and brush head wear, an advertising identifier, account data and, for users who opt in, data shared with an online retailer, a dental insurer and a dental supplier. Children may use the same app through a parent’s account.

C1 affects every user who relied on the Data Safety section. H1 affects the first seconds of every launch. H2 affects every user outside China who tries to exercise a right. H3 and L1 concern the position of minors. M1 to M3 concern identifiers, credentials and a broad calendar permission.

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

The Complete Chain

Step 1, store: the Data Safety section says no data is shared with third parties (C1).

Step 2, install and first launch: FirebaseInitProvider starts at initOrder 100 with the process, and no Analytics override exists (H1).

Step 3, onboarding: the consent text names Adobe, Apptentive, Branch and Firebase Crashlytics and says Branch collects the Android Advertiser ID. The ad services configuration is open to all attribution partners (C1, M1).

Step 4, use: brushing, reorder data and optional sharing with Amazon, Delta Dental and Henry Schein. A Kids handle appears in the product configuration (H3). The calendar permission opens every calendar for reminders (M3).

Step 5, the user acts on a right: the only link in the notice leads to philips.com.cn and no Union representative is named (H2).

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1, H1, H2 and H3.

Article 5(1)(c), data minimisation: engaged by H3, L1 and M3.

Article 6(1) and Article 7(1), lawful basis and conditions for consent: engaged by C1, H1 and M1, because processing that starts before a consent decision has no consent to rest on.

Article 8, child's consent: engaged by H3 and L1.

Article 12(2), facilitating the exercise of rights: engaged by H2.

Article 13(1)(a), (b) and (e), identity and contact details of the controller, contact details of a representative, recipients: engaged by H2 and C1.

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

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

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

Article 33(4), notification in phases, was quoted in the notice. The report makes no finding under Article 33.

Consumer Protection & Platform Disclosures

The Google Play Data Safety section, read on 2026-08-22, says the app may collect Personal info, Health and fitness and 4 other types, encrypts data in transit, and shares no data with third parties. It also says data deletion can be requested, which is consistent with the in-app deletion feature. The listing rates the app PEGI 3 and Health and Fitness. The sharing statement is the one that C1 sets against the package. The definition of sharing in Google's own guidance is the main reason for the rating basis in C1.

Regulatory & Legal Landscape

The framework applied is the GDPR, with Article 27 for a controller outside the Union, Article 8 for children and Article 5(1)(a) for transparency. The operator is established in the USA and offers its product to users in Austria, which brings Article 3(2) GDPR into play.

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 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 where the source holds them in full.

```
Package            com.philips.cdp.ohc.tuscany
Version            10.20.0 (versionCode 254), analysed 2026-08-22
base.apk SHA-256   c9ae8c8077d1dc1f2c11443f80a3ace658465c9afc3d1c2251b99c519a072375
XAPK SHA-256       f798fbb105a66138963faf6a17e11c8b56e6010294eb4468af26197375d13576
minSdk / targetSdk 31 / 36

Firebase project   ph-ohc-sonicare
google_api_key     AIzaSyAKwcJy9SUiCDxtJjx9Q6Yu26-a2ou6Tio
google_app_id      1:196989047715:android:788f3456b22f61c3418016
Storage bucket     ph-ohc-sonicare.appspot.com
web client id      196989047715-rqm7f4enmiev8bgquh70mdn6gmid3hd1.apps.
    googleusercontent.com

LWA clientId       amzn1.application-oa2-client.9421e1db14e341d5adfc3e7bb3ca8e86
LWA appFamilyId    amzn1.application.a738afd4b80b4b3c9df765a5999e1448
LWA appsigSha256   D2:D6:95:A1:1D:1B:84:F9:25:A9:45:6E:27:F4:45:E9:FD:87:C3:74:63:AA:8
    A:34:32:A6:6A:23:3B:0F:D5:0F
ProductRegistration IQytAjOkX43QmYQ0R7MiG9vJzQX9evBJ2kZEPKgU
PIL_ECommerce_API_KEY yaTmSAVqDR4GNwijaJie3aEa3ivy7czu22BxZwKP
PIM apiKey CN       IRZthgIyd72LE39zqoRsW5TZ6MMOnFEV9LDfFwRs
PIM apiKey RU       ochuwzHTrQax4IQiWQn3m9JJab70ETP29L3xUAtY
PIM apiKey default  xpbccXhsgr4J9h6eFzznq9JYz2Ag7sGl5awGL4Xq
weChatAppId        wx53fa669d65050e61
```

```
C1  assets/html/privacy_policy_summary.html, res/values/strings.xml (
    NEW_ONBG_ANALYTICS_NOTICE, DART_EXP_SET_REORDER_CONSENT,
    DELTA_DENTAL_CONSENT_TEXT, HENRY_SCHEIN_CONSENT_TEXT), classes*.dex
H1  AndroidManifest.xml: FirebaseInitProvider initOrder 100, no
    firebase_analytics_collection_enabled
H2  assets/html/privacy_policy_summary.html: controller paragraph and Contact Us link
H3  assets/ProductsConfiguration_*.json (57 market files, 9 sampled), res/values/
    strings.xml
M1  AndroidManifest.xml, res/xml/ga_ad_services_config.xml
M2  res/values/strings.xml, assets/api_key.txt, assets/AppConfig.json
M3  AndroidManifest.xml: READ_CALENDAR, classes*.dex: CalendarContract
L2  AndroidManifest.xml, assets/PrivacyNotice.json, assets/AppConfig.json
```

Reproduction: obtain com.philips.cdp.ohc.tuscany 10.20.0 from Google Play, check the SHA-256 above, decode the manifest and resources with apktool, unzip the assets and read the named files. No device, account or network access is needed.

Disclosure Timeline & Outcome

2026-08-22 12:04 UTC Notice REF SONICARE-2026-R1 to OHCAppSupport@philips.com and privacy@philips.com, CC DSB and EDPS. Findings C1, H1, H2, H3 in the text, three further findings summarised, three questions asked.

2026-10-17 18:51 UTC Follow-up from security@rfi-irfos.com to the same addresses, 34 days before the embargo date, with the open findings and the same three questions.

2026-11-15 12:56 UTC Second follow-up from security@rfi-irfos.com to the same addresses, five days before the embargo date, with the open findings and the same three questions.

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

2026-11-21 Publication of this report. No reply of any kind has been received, including no automatic acknowledgement, and no delivery failure was returned.

What Philips Got Right

Cleartext traffic is denied by usesCleartextTraffic false, and the network security configuration allows no cleartext carve-out, only a standard debug override that does not affect release builds. data_extraction_rules.xml excludes root, file, database, sharedpref and external data from cloud backup and device transfer, and allowBackup is false. BLUETOOTH_SCAN carries neverForLocation. No RECORD_AUDIO and no CAMERA permission is requested. A regional consent table in PrivacyNotice.json decides which consent flows apply per market. The WeChat and Tencent functionality is gated to Taiwan, Macau, Hong Kong and Mainland China. A self-service account deletion exists and is described in the notice with a processing time of fifteen days. The Firebase disclosure names Google Ireland Ltd. and lists the identifiers, which is more precise than generic wording. The app shows no advertising and the dex files hold no ad mediation SDK.

Residual Risk & Recommendations

Open on 21 November 2026: all nine items, with no written position from the operator. Items that only the operator can close are the Data Safety correction or classification in C1, the analytics override in H1, the Union contact and representative in H2, the Kids handle question in H3 and the server side scope of the credentials in M2.

Recommendations: align the Data Safety section with the Privacy Notice, set firebase_analytics_collection_enabled to false and enable collection after consent, name a Union representative and a working rights channel, state whether Kids handles pair in this app, restrict the attribution configuration to named partners, move or rotate the credentials, and request only the calendar permission that is needed.

This final 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

plus public documents read from the public sites. No Philips servers or accounts were probed. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. REF SONICARE-2026-R1.