# Security & Privacy Disclosure, Final Report

## Oclean Care+ for Android (com.yunding.noopsychebrushforeign)

Every question answered in writing, two code fixes verified, controller, EU representative and EEA processor published.

**PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO DATE 20 NOVEMBER 2026 REACHED. STATE PER RFI-IRFOS RECORDS, LAST RECORDED EXCHANGE 23 OCTOBER 2026.**

| | |
|---|---|
| **Target** | Shenzhen Yunding Information Technology Co., Ltd. (Oclean) |
| **Versions Audited** | 4.0.4 / 114 (2026-08-22) · 4.0.7 / 117 (2026-09-18, 2026-10-19) |
| **EU Representative** | OCLEAN CARE TECHNOLOGY SP Z O.O., Warsaw |
| **Notice / Publication** | 2026-08-22 / 2026-11-20 (90 days, unchanged) |
| **Findings** | 8: 2 High, 4 Medium, 2 Low (C1 reassessed from Critical) |
| **Status** | Per RFI-IRFOS records: 4 remediated (H2 vendor-reported), 4 committed for v4.0.9, no final APK diff on record |
| **SHA-256 (base APK)** | `b21c497502b7df1f929ac00354d5e13532851e01a2f14003334c16909d333323` |

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 6

4 Architecture & Data Flow 6

5 Engagement Summary 7

6 Findings 7

6.1 C1: Hardcoded first-party hosts on Hangzhou-registered infrastructure, no storage location or processor disclosed . . . 7

6.2 H1: No controller identity, no DPO, no Article 27 representative in any consulted source . . . 8

6.3 H2: No consent management, single blanket checkbox, Firebase auto-initialised before any consent screen . . . 9

6.4 M1: No network security config, app-wide cleartext permitted, contradicting the Play label encrypted in transit . . . 10

6.5 M2: Unstripped iFlytek speech SDK sample project with face and voiceprint 1:N identification demo modules . . . 10

6.6 M3: Firebase API key and project identifiers hardcoded (project oclean-216010) 11

6.7 L1: Date of birth collected without an age gate or parental consent path . . . 11

6.8 L2: allowBackup true with backup and data-extraction rules that exclude nothing 12

7 Impact Analysis 12

8 The Complete Chain 13

9 Data Protection: Article by Article 13

10 Consumer Protection & Platform Disclosures 14

11 Regulatory & Legal Landscape 14

12 Indicators of Compromise & Reproducible Evidence 15

13 Disclosure Timeline & Outcome 16

14 What Oclean Got Right 17

15 Factual-Accuracy Review 17

16 Residual Risk & Recommendations 17

## Executive Summary

Oclean Care+ is the Bluetooth companion app for Oclean smart electric toothbrushes, published on Google Play by Shenzhen Yunding Information Technology Co., Ltd. with more than 500,000 installs. On 22 August 2026 RFI-IRFOS disclosed eight findings from a static root-level analysis of version 4.0.4 under REF OCLEAN-2026-R1. The two most serious concerned the app's own backend: first-party hostnames hardcoded in the binary resolved to Alibaba Cloud infrastructure registered in Hangzhou, China, while neither the app nor its privacy policy named a controller, an EU representative, a processor or a storage location.

Oclean answered every question in writing within 25 days of the first notice and kept answering until each one was closed. It named Shenzhen Yunding Information Technology Co., Ltd. as controller and OCLEAN CARE TECHNOLOGY SP Z O.O. in Warsaw as its Article 27 representative. It identified hwapi3.oclean.com and hwapicore.oclean.com as the hosts serving EU users and supplied DNS and instance evidence that both run in Alibaba Cloud's Frankfurt region, which RFI-IRFOS verified independently. It published Alibaba Cloud as its Article 28 processor for EEA users in the privacy policy the app loads, and it shipped version 4.0.7 with a strict network security configuration and with the bundled iFlytek biometric sample project removed.

The case also records a correction by RFI-IRFOS. Our message of 18 September 2026 wrongly stated that hwapi3.oclean.com and hwapicore.oclean.com resolved to Hangzhou. Our own first notice had already recorded them in the ALICLOUD-DE block. We corrected the statement in writing on 21 September 2026 and credited the routing question as answered. On the evidence now available, EU personal data reaches Frankfurt, and the original critical rating of C1, which rested on an undisclosed transfer to China, is reassessed in this report to the transparency gap that was actually demonstrated.

On 23 October 2026 Oclean reported its remediation status in writing: the web-shop policy updated, Firebase initialisation before consent remediated in v4.0.8, and the asset host change, App Check, the age gate and the backup rules committed for v4.0.9. Per RFI-IRFOS records the last exchange is that of 23 October 2026, and no final APK diff is on record, so the states above are those of that date. This case is the clearest example in the programme of a company turning a disclosure into a sequence of verifiable fixes.

**Scope:** Static root-level analysis of the Google Play release binaries 4.0.4 (versionCode 114) and 4.0.7 (versionCode 117): manifest, resources, dex string pool, native libraries. Passive public DNS and WHOIS lookups on hostnames hardcoded in the binary. Public web pages read by plain HTTP GET: the Play Store listing and Data Safety page, oclean.com legal pages, and the privacy policy at hwapi3.oclean.com. No backend API was called, no account was created, no traffic was intercepted, and no runtime instrumentation was used.

| ID | Severity | Title |
|---|---|---|
| C1 | MEDIUM | Hardcoded first-party hosts on Hangzhou-registered infrastructure, no storage location or processor disclosed |
| H1 | HIGH | No controller identity, no DPO, no Article 27 representative in any consulted source |
| H2 | HIGH | No consent management, single blanket checkbox, Firebase auto-initialised before any consent screen |
| M1 | MEDIUM | No network security config, app-wide cleartext permitted, contradicting the Play label encrypted in transit |
| M2 | MEDIUM | Unstripped iFlytek speech SDK sample project with face and voiceprint 1:N identification demo modules |
| M3 | MEDIUM | Firebase API key and project identifiers hardcoded (project oclean-216010) |
| L1 | LOW | Date of birth collected without an age gate or parental consent path |
| L2 | LOW | allowBackup true with backup and data-extraction rules that exclude nothing |

| ID | Disclosed | This report | Status on 23 October 2026 |
|---|---|---|---|

## Finding Status at a Glance

| ID | Disclosed | This report | Status on 23 October 2026 |
|---|---|---|---|
| C1 | CRITICAL | MEDIUM | Answered. EU data verified in Frankfurt, processor and location disclosed since 22 Sep 2026, sdkauth and test hosts removed in 4.0.7. Asset host change committed for v4.0.9. |
| H1 | HIGH | HIGH | Remediated in the in-app policy. Web-shop policy reported updated by Oclean on 23 Oct 2026. |
| H2 | HIGH | HIGH | Reported remediated in 4.0.8 by Oclean on 23 Oct 2026. Runtime gating confirmed in the final diff. |
| M1 | MEDIUM | MEDIUM | Fixed and verified in 4.0.7 on 18 Sep 2026. |
| M2 | MEDIUM | MEDIUM | Fixed and verified in 4.0.7 on 18 Sep 2026, five independent locations. |
| M3 | MEDIUM | MEDIUM | Accepted. App Check SDK committed for v4.0.9, enforcement after 95 percent adoption. |
| L1 | LOW | LOW | Open in 4.0.7. Age gate and parental authorisation workflow committed for v4.0.9. |
| L2 | LOW | LOW | Open in 4.0.7. Backup rules fix committed for v4.0.9. |

## Subject & Operator Analysis

Google Play lists the app under Shenzhen Yunding Information Technology Co., Ltd. At the time of the first notice this developer field was the only place the operator was identified. The app's string table, the privacy policy at oclean.com/pages/privacy-policy and the terms of service at oclean.com/policies/terms-of-service named no legal entity, no address, no DPO and no EU representative.

Oclean's written replies of 16 and 17 September 2026 closed that gap. Shenzhen Yunding Information Technology Co., Ltd. is the sole controller for EU users. OCLEAN CARE TECHNOLOGY SP Z O.O., UL. JANISZOWSKA 8, PL-02-264 Warszawa, is the Article 27 representative under a written mandate that entered into force on 7 September 2026. The Compliance Lead, Tina Ba, signed for Oclean Care Technology (Shenzhen) Co., Ltd. and named Xianghui Lu (luxh@oclean.com) as technical contact.

On 19 October 2026 the privacy policy loaded by the app from hwapi3.oclean.com names Shenzhen Yunding Information Technology Co., Ltd. with a registered address in Nanshan District, Shenzhen, names the Warsaw representative, and names Alibaba Cloud as processor for EEA users on servers in Frankfurt. The Shopify privacy policy at oclean.com/pages/privacy-policy, the page checked at the first notice, still names none of these on the same date. That page serves the web shop, and the app does not link to it in 4.0.7.

## Architecture & Data Flow

Oclean Care+ is a native Kotlin and Java app with a single main dex file, a small native footprint (Tencent MMKV for local storage plus two image utilities) and no third-party ad mediation. The toothbrush pairs over Bluetooth Low Energy with BLUETOOTH_SCAN flagged neverForLocation. Account data, brushing records, family-space membership and profile data travel to Oclean's own backend.

The backend is selected on the client by mobile country code. Oclean's technical document of 16 September 2026 defines three buckets: AGENT_BM for North America, AGENT_TW for Taiwan, and AGENT_HW for every other country, including all EU member states. On 20 September 2026 Oclean identified AGENT_HW as hwapi3.oclean.com and hwapicore.oclean.com. Both resolve to 8.209.75.125 in the ALICLOUD-DE block, Alibaba Cloud's Frankfurt region, which RFI-IRFOS confirmed by DNS and WHOIS on 21 September 2026. bmapi3.oclean.com and bmapicore.oclean.com serve North America from Alibaba Cloud LLC address space.

Three hostnames in 4.0.4 resolved to Aliyun Computing Co., LTD in Hangzhou. sdkauth.oclean.com and test.oclean.com were legacy test hosts according to Oclean and are absent from 4.0.7. care.oclean.com remains once, as care.oclean.com/three/, and serves the static three.js scene and a single .dae model for the animated brushing view. Firebase (project oclean-216010) provides messaging and crash reporting.

## Engagement Summary

The first notice went to service@oclean.com and guozr@oclean.com on 22 August 2026, with the Austrian DSB and the EDPS in copy. guozr@oclean.com returned a permanent 550 failure within seconds. Two follow-ups went out on 12 September 2026.

Oclean's compliance team replied on 16 September 2026 with two formal, point-by-point letters, accepted the transparency, consent and network findings as stated, explained the iFlytek bundle as an unstripped build artefact, and committed to 30-day and 60-day remediation windows. Every later exchange narrowed the open points: the Article 27 mandate (answered 17 September), the Firebase controls (answered 17 September), the EU routing hostname (answered 20 September with DNS and instance evidence), and the public naming of the processor (answered 22 September, verified live on 17 October).

RFI-IRFOS verified fixes against the shipped binary instead of accepting them on assertion: 4.0.7 was pulled from a live device on 18 September 2026 and checked for M1 and M2 across five independent locations each. The one error in the exchange was ours, corrected in writing three days after it was made.

## Findings

### C1: Hardcoded first-party hosts on Hangzhou-registered infrastructure, no storage location or processor disclosed

**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 CRITICAL on 22 August 2026, reassessed after verification**

Disclosed as CRITICAL because three hardcoded first-party hostnames in 4.0.4 (care.oclean.com, sdkauth.oclean.com, test.oclean.com) resolved per public WHOIS to Aliyun Computing Co., LTD in Hangzhou, and the privacy policy named no third country, processor or transfer mechanism. Oclean showed, and RFI-IRFOS verified on 21 September 2026, that EU traffic uses hwapi3.oclean.com and hwapicore.oclean.com in Alibaba Cloud Frankfurt. The undisclosed transfer to China is therefore not demonstrated for EU personal data. The demonstrated finding is the transparency gap plus PRC-hosted legacy hosts in a release binary, rated here on that basis.

```
4.0.4 (2026-08-22)
care.oclean.com       182.92.251.147   Aliyun Computing Co., LTD, Hangzhou, CN
sdkauth.oclean.com    60.205.83.153    Aliyun Computing Co., LTD, Hangzhou, CN
test.oclean.com       123.56.108.247   Aliyun Computing Co., LTD, Hangzhou, CN
bmapi3/bmapicore      47.88.92.203     Alibaba Cloud LLC (North America bucket)
hwapi3/hwapicore      8.209.75.125     ALICLOUD-DE, Frankfurt (EU and rest-of-world
    bucket)

4.0.7 (2026-09-18 and 2026-10-19)
sdkauth.oclean.com, test.oclean.com   absent from the binary
care.oclean.com/three/                static three.js scene and .dae model only
```

Remediation: the privacy policy loaded by the app has named Alibaba Cloud as Article 28

processor for EEA users on Frankfurt servers since 22 September 2026, verified live on 17 and 19 October 2026.

**Impact:** Until 22 September 2026 an EU user reading the app's privacy notice could not learn where account data was stored or which processor held it, and the release binary carried live hostnames on Hangzhou infrastructure that Oclean itself described as test leftovers.

**Fix:** Done for the disclosure and for two of three hosts. Serving the care.oclean.com/three/ assets from the Frankfurt region would remove the last Hangzhou-hosted first-party host from the binary. On 23 October 2026 Oclean stated that the 3D model assets will load through the AndroidX WebViewAssetLoader on a virtual HTTPS domain that resolves to no server, planned for v4.0.9. This is a vendor statement and is checked in the final diff.

**H1: No controller identity, no DPO, no Article 27 representative in any consulted source**

---

**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), rated HIGH by blast-radius escalation, remediated**

RFI-IRFOS blast-radius escalation: CVSS scores technical exploitability and gives a pure transparency failure 0.0. Rated HIGH because more than 500,000 users of a health-adjacent app had no way to identify who processed their data or whom to address a GDPR request to, which disables every other data-subject right. At the first notice, 1,900+ app strings, the privacy policy, the terms of service and the contact page named no legal entity, no address, no DPO and no EU representative.

Remediation: Oclean named the controller and the Warsaw representative in writing on 16 September 2026 and confirmed the mandate in force since 7 September 2026. The in-app privacy policy names both on 19 October 2026.

**Impact:** Users could not exercise access, erasure or objection rights against an identified controller, and EU supervisory authorities had no EU point of contact for the app.

**Fix:** Done in the in-app policy. Aligning the oclean.com web-shop policy with the same controller and representative details would close the last place where they are missing. On 23 October 2026 Oclean stated that the privacy policy at oclean.com/pages/privacy-policy has been updated. This is a vendor statement and is checked in the final diff.

### H2: No consent management, single blanket checkbox, Firebase auto-initialised before any consent screen

**MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 5.1 (CVSS-B), rated HIGH by blast-radius escalation, remediation observed in 4.0.7, reported remediated in 4.0.8**

RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.1 to HIGH because the defect applied to every user on every cold start, regardless of jurisdiction, and because consent was the only legal basis the app offered for its processing. In 4.0.4 the whole consent flow was one checkbox, I have read and agree, bound to a combined registration agreement and privacy policy, and FirebaseInitProvider (initOrder 100, directBootAware) started before any screen could render.

```
4.0.4  provider FirebaseInitProvider  initOrder=100  directBootAware=true
4.0.7  no FirebaseInitProvider declared
4.0.7  meta-data firebase_analytics_collection_enabled = false
4.0.7  strings: login_privacy_setting_title  "Privacy Settings"
               login_privacy_setting_must_need  "Basic essential services"
               login_privacy_setting_push  "Push notifications"
               login_privacy_setting_google_login_tip  (cross-border notice for Google
    login)
```

Oclean committed on 16 September 2026 to granular per-purpose consent and to Firebase initialisation after consent within 60 days. The 4.0.7 binary already shows both changes at manifest and resource level. Whether initialisation is gated at runtime was not tested and is checked in the final diff.

**Impact:** Under 4.0.4 a user's device contacted Google's Firebase services before the user had seen any choice, and the only choice later offered bundled account creation with every processing purpose.

**Fix:** Oclean stated on 23 October 2026 that automatic Firebase initialisation before consent was remediated in v4.0.8 and will be kept in later releases. The 4.0.8 build is checked at runtime in the final diff. Analytics collection stays disabled until the matching toggle is on.

### M1: No network security config, app-wide cleartext permitted, contradicting the Play label encrypted in transit

**MEDIUM, CVSS v4.0 AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 6.0 (CVSS-B), fixed and verified**

4.0.4 set android:usesCleartextTraffic to true at application level and shipped no network_security_config.xml at all, with no domain scoping and no pinning, while the Play Data Safety label stated that data is encrypted in transit. Oclean confirmed the finding on 16 September 2026.

```
android:usesCleartextTraffic="false"
android:networkSecurityConfig="@xml/network_security_config"
base-config denies cleartext, scoped domain-config, pinned trust anchor
no debug-overrides trusting user certificates
no TrustManager with an empty checkServerTrusted
```

**Impact:** Any request built with an http URL could have left the device unencrypted on a shared network, with account and location data in reach of anyone on the same Wi-Fi.

**Fix:** Done in 4.0.7.

### M2: Unstripped iFlytek speech SDK sample project with face and voiceprint 1:N identification demo modules

**LOW, CVSS v4.0 AV:L/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.1 (CVSS-B), rated MEDIUM by blast-radius escalation, fixed and verified**

RFI-IRFOS blast-radius escalation: raised from LOW/2.1 to MEDIUM because the bundle carried biometric identification scaffolding and cleartext PRC endpoints in a release distributed to more than 500,000 users, next to an app-wide cleartext allowance (M1), so activation would have needed no further engineering. 4.0.4 contained iFlytek attribution text, settings screens for dictation, evaluation, synthesis and semantics, the endpoints bj.voicecloud.cn, gz.voicecloud.cn, dx.xf-yun.com and aiui.xfyun.cn, and demo titles for face and voiceprint 1:N identification. No iFlytek class was found in the dex code, and the finding was disclosed as a build-hygiene finding from the start.

Verified absent in 4.0.7 on 18 September 2026 across the dex string pool, resources.arsc, the res/xml preference screens, the machine_entries and machine_values arrays, and the native library set. iat_setting.xml, ise_settings.xml, tts_setting.xml, understand_setting.xml and url_setting.xml no longer exist.

**Impact:** A dormant third-party biometric capability sat in the phones of every user with a ready network path to servers in China, which Oclean confirmed was an oversight in its overseas build pipeline.

**Fix:** Done in 4.0.7, with automated pre-release scanning added to the build gate according to Oclean.

### M3: Firebase API key and project identifiers hardcoded (project oclean-216010)

**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), accepted**

The key AIzaSyAmbmJpvV0UgvLEJM7rNfl7zgRROvXoG9c, sender ID 408154414872, app ID 1:408154414872:android:3f6cb440b6f5c58951486d and bucket oclean-216010.appspot.com ship in the binary, in 4.0.7 as well. Firebase keys are client identifiers by design. The finding is the burden of proof on backend restriction.

Oclean confirmed on 17 September 2026 that Security Rules are deny-by-default for this project and that App Check runs in observation mode with token injection in the CI pipeline. Enforcement mode was not active on that date.

**Impact:** Anyone holding the key can attempt quota exhaustion or rule probing against the project, contained by the deny-by-default rules Oclean confirmed.

**Fix:** Accepted. On 23 October 2026 Oclean committed to integrate the App Check SDK in v4.0.9 and to enable enforcement once more than 95 percent of users run v4.0.9 or newer, because immediate enforcement would break existing installations.

### L1: Date of birth collected without an age gate or parental consent path

**LOW, CVSS v4.0 AV:N/AC:L/AT:P/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B), open, remediation committed for v4.0.9**

Onboarding asks Please enter your date of birth, and the family space lets members see each other's brushing status. No string references a minimum age, a parental-consent flow or differentiated handling of minors. The DOB strings are unchanged in 4.0.7.

**Impact:** A toothbrush coaching app used by families knows when a user is a child and applies no protective handling on that basis.

**Fix:** On 23 October 2026 Oclean stated that a new solution is finalised and will ship in v4.0.9. Use the collected date of birth to route users under the national age of digital consent through a parental consent step, or stop collecting it.

### L2: allowBackup true with backup and data-extraction rules that exclude nothing

**LOW, CVSS v4.0 AV:P/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 1.0 (CVSS-B), open, remediation committed for v4.0.9**

backup_rules.xml contains an empty full-backup-content element and data_extraction_rules.xml an empty cloud-backup element, so the entire private data directory, including the MMKV store, is eligible for device-to-device and cloud backup. Unchanged in 4.0.7.

**Impact:** Session material and family-space data can leave the app sandbox through backup channels the user does not associate with Oclean.

**Fix:** On 23 October 2026 Oclean stated that this will be remediated in v4.0.9. Exclude the MMKV directory and token storage in both rule files, or set allowBackup to false.

## Impact Analysis

The people affected are households who bought an Oclean toothbrush and installed the companion app to use it. The app is rated PEGI 3, collects date of birth, and has a family space in which several members share brushing status, so children are among its users by design. The product is a paid device. The app carries no ad mediation, which removes the usual argument that data pays for a free service, and makes clear disclosure of where that data goes the more important.

At the first notice these users could not learn who processed their data, where it was stored, or which processor held it (C1, H1). Their only consent choice was a single checkbox, and Firebase started before they saw it (H2). Requests could leave the device unencrypted (M1), and a dormant biometric sample project with cleartext endpoints in China sat in the binary (M2).

On the evidence verified by this report, their account data was stored in Frankfurt throughout. The harm demonstrated was a harm of opacity and of default configuration: users had no means to verify what this report now verifies, and no notice that let them exercise their rights against a named controller.

## The Complete Chain

Step 1, purchase and install: a household buys an Oclean toothbrush and installs Oclean Care+ from Google Play, where the developer field reads Shenzhen Yunding Information Technology Co., Ltd. and the Data Safety label states that data is encrypted in transit.

Step 2, first launch: in 4.0.4 FirebaseInitProvider starts with the process, before any screen (H2).

Step 3, registration: the user ticks I have read and agree for a combined registration agreement and privacy policy that names no controller, no representative, no processor and no storage location (H1, C1). The app asks for date of birth and offers a family space (L1).

Step 4, transmission: the client picks a backend by mobile country code. EU devices fall into AGENT_HW and reach hwapi3.oclean.com and hwapicore.oclean.com in Frankfurt. The binary also carries hostnames on Hangzhou infrastructure and permits cleartext traffic app-wide (C1, M1).

Step 5, on the device: a third-party biometric sample project with endpoints in China sits unused in the package (M2), and app data is eligible for full backup (L2).

Step 6, the user tries to act: before 16 September 2026 no document gave the user a controller or EU address to write to. Since 22 September 2026 the in-app policy names the controller, the Warsaw representative and the Frankfurt processor, and since 4.0.7 steps 2, 4 and 5 are closed or closing in code.

## Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1, H1 and M1 at disclosure. The Play label and the binary contradicted each other, and the policy named no controller. Addressed by the policy update and by 4.0.7.

Article 7 and Article 4(11), conditions for consent: engaged by H2. A single bundled checkbox does not give specific, informed consent per purpose. Oclean accepted this in writing on 16 September 2026.

Article 8, child's consent: engaged by L1. Date of birth is collected without any age-dependent handling.

Article 13(1)(a) and (b), identity of controller and DPO contact: engaged by H1, now met in the in-app policy. Oclean stated on 16 September 2026 that a DPO is not mandatory under Article 37 and that its compliance team performs the function. The in-app policy states that Oclean set up a DPO reachable at service@oclean.com. Both statements are recorded as made.

Article 13(1)(e) and (f), recipients and third-country transfers: engaged by C1. The processor and the Frankfurt location are now named. The policy also states that personal information may be stored anywhere in the world and lists data centres in China, Germany, Russia, Singapore and the United States, a general clause that sits alongside the EEA-specific paragraph.

Article 25, data protection by design and by default: engaged by M2, M3 and L2.

Article 27, EU representative: engaged by H1. Met since 7 September 2026.

Article 28, processor: Alibaba Cloud named with Article 28 agreements in place according to the policy.

Article 32, security of processing: engaged by M1, M3 and L2. M1 fixed.

Articles 44 and 46, transfers: raised by C1 at disclosure. On the verified routing, EU personal data stays in the EU, and no transfer finding is asserted.

## Consumer Protection & Platform Disclosures

The Google Play Data Safety label for the app stated on 22 August 2026 that data is encrypted in transit and that no data is shared with third parties. The 4.0.4 binary permitted cleartext traffic app-wide (M1) and initialised Firebase before consent (H2). A label a consumer relies on when choosing a connected device app contradicted the shipped configuration. Oclean committed on 16 September 2026 to align the Data Safety declaration with the updated policy. The current label is checked again in the final diff before publication.

## Regulatory & Legal Landscape

Shenzhen Yunding Information Technology Co., Ltd. has no EU main establishment, so the one-stop-shop mechanism does not apply and every supervisory authority in whose territory users are affected is competent under Article 3(2) and Article 55. The Austrian Datenschutzbehörde and the European Data Protection Supervisor received the first notice in copy. The Polish UODO is the authority where the Article 27 representative sits.

Among the smart-toothbrush companion apps in the RFI-IRFOS corpus, Oclean Care+ was the first with a PRC-based operator and, at disclosure, the weakest transparency posture. It is also the one where the operator moved furthest within the 90 days, from no named entity to a named controller, representative and processor, and from no network security configuration to a pinned one.

## Indicators of Compromise & Reproducible Evidence

Every point below is reproducible from the public Google Play builds and public DNS and WHOIS.

```
Package       com.yunding.noopsychebrushforeign
4.0.4 / 114   base.apk SHA-256
    b21c497502b7df1f929ac00354d5e13532851e01a2f14003334c16909d333323
              XAPK     SHA-256 7
    bf073c26e2a1d7cfd9288743493f1ba179da8d536aa5d912509251090de7451
4.0.7 / 117   base.apk SHA-256 12538804759
    daac53982a8834e28d26e4428fee8e94187b315ccce82447fcf7a
Firebase      project oclean-216010, sender 408154414872
              app 1:408154414872:android:3f6cb440b6f5c58951486d
```

```
hwapi3.oclean.com, hwapicore.oclean.com   8.209.75.125     ALICLOUD-DE, Frankfurt
bmapi3.oclean.com, bmapicore.oclean.com   47.88.92.203     Alibaba Cloud LLC
care.oclean.com                           182.92.251.147   Aliyun Computing Co., LTD,
    Hangzhou
sdkauth.oclean.com (4.0.4 only)           60.205.83.153    Aliyun Computing Co., LTD,
    Hangzhou
test.oclean.com (4.0.4 only)              123.56.108.247   Aliyun Computing Co., LTD,
    Hangzhou
bj.voicecloud.cn, gz.voicecloud.cn, dx.xf-yun.com, aiui.xfyun.cn (4.0.4 only, iFlytek)
```

```
In-app policy  https://hwapi3.oclean.com/shopping/xieyi/ocxy_yszc_en.html  (checked
    2026-10-17, 2026-10-19)
Web shop       https://www.oclean.com/pages/privacy-policy  (checked 2026-08-22,
    2026-10-19)
```

## Disclosure Timeline & Outcome

2026-08-22 First notice (REF OCLEAN-2026-R1) to service@oclean.com and guozr@oclean.com, CC Austrian DSB and EDPS. guozr@oclean.com bounced permanently (550).

2026-09-12 Two follow-ups to service@oclean.com restating the findings and the three questions.

2026-09-16 Two formal replies from Oclean's compliance team: controller and Article 27 representative named, NSC and consent findings accepted, iFlytek bundle explained and removed from the pipeline, 30-day and 60-day remediation windows committed. RFI-IRFOS replied the same day, confirming four points and asking three open questions (OPEN-1 to OPEN-3).

2026-09-17 Oclean answered OPEN-1 (mandate in force since 7 September 2026) and OPEN-3 (Security Rules deny-by-default, App Check in observation mode), and attached its region-identification document for OPEN-2.

2026-09-18 RFI-IRFOS pulled 4.0.7 from a live device and verified M1 and M2 as fixed. The same message wrongly stated that hwapi3.oclean.com and hwapicore.oclean.com resolved to Hangzhou.

2026-09-20 Oclean identified the AGENT_HW hosts and supplied DNS and Alibaba Cloud instance evidence for Frankfurt.

2026-09-21 RFI-IRFOS corrected its 18 September statement in writing, verified Frankfurt independently, credited OPEN-2 as answered, and asked whether the public policy would name the processor.

2026-09-22 Oclean published Alibaba Cloud as Article 28 processor in the in-app privacy policy.

2026-10-17 RFI-IRFOS verified the policy paragraph live.

2026-10-19 Oclean requested a factual-accuracy review. This preliminary report issued to Oclean.

2026-10-23 Oclean reported its remediation status: H1 and the web-shop policy updated, H2 remediated in v4.0.8, and C1, M3, L1 and L2 committed for v4.0.9.

2026-11-20 Embargo date, unchanged since 22 August 2026.

2026-11-21 Published. Per RFI-IRFOS records no message from Oclean after 23 October 2026 is on record.

## What Oclean Got Right

Oclean replied with named people, dates and documents, and each reply answered the question asked. It accepted findings it could have contested, including the consent finding, and it supplied verifiable evidence where it disagreed, which is how the routing question was settled. It fixed two findings in shipped code within four weeks and published its controller, representative and processor in the notice its users actually see. The app itself carries no ad mediation, no PRC analytics or push SDKs, scans for the toothbrush without location access, and offers real in-app account deletion.

## Factual-Accuracy Review

RFI-IRFOS shares a preliminary report before publication only with companies whose every finding has been answered or remediated, and only for a factual-accuracy check. Oclean qualified on 19 October 2026 and received the draft of this report on that date. Corrections of fact (a version, a hostname, a date, an attribution) are accepted with evidence until 13 November 2026 and listed below in the published version. Severity ratings, assessments and the publication date are not part of the review. Per RFI-IRFOS records, no final APK diff was run before publication.

Corrections accepted: none are recorded in RFI-IRFOS records as of 21 November 2026.

Final APK diff: none is recorded in RFI-IRFOS records, so remediation states are those reported by Oclean on 23 October 2026 and are stated by the operator, not verified by RFI-IRFOS.

## Residual Risk & Recommendations

Open at the date of publication, per RFI-IRFOS records: L1 (date of birth without an age gate) and L2 (backup rules that exclude nothing), both unchanged in 4.0.7 and committed by Oclean for v4.0.9. Partial: App Check in observation mode (M3), committed for v4.0.9, and runtime confirmation of the consent gating that Oclean reports as shipped in v4.0.8 (H2).

Consistency points for Oclean's own documents: the in-app policy lists data centres in China, Russia, Singapore and the United States and says data may be stored anywhere in the world, next to the EEA paragraph naming Frankfurt. The policy names a DPO, while the letter of 16 September 2026 states that none is mandatory. The oclean.com web-shop policy names no controller or representative. The Play Data Safety label should match the policy.

Recommendations: gate Firebase at runtime behind the new privacy settings, enforce App Check, use the date of birth for an age-appropriate consent path or drop it, exclude token and MMKV storage from backup, and serve the care.oclean.com/three/ assets from Frankfurt so no first-party host in the binary points to Hangzhou.

**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 Static root-level analysis of the published application plus passive public DNS and WHOIS. No Oclean servers or accounts were probed. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. REF OCLEAN-2026-R1.