Security & Privacy Disclosure, Final Report

Oral-B App for Android (com.pg.oralb.oralbapp)

A toothbrush app whose US legal text calls brushing data health data for advertising, while its EU consent text never uses the word.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO DATE 20 NOVEMBER 2026 REACHED. THREE POINTS REMAIN OPEN, NO REPLY TO THE FOLLOW-UPS AS OF 21 NOVEMBER 2026.

Target	Procter & Gamble Service GmbH, Schwalbach am Taunus, Germany (controller named in the app for Germany, Austria and Switzerland)
Versions Audited	10.8.0 / 13821 (analysed 2026-08-21, notice 2026-08-22)
Notice / Publication	2026-08-22 / 2026-11-20 (90 days)
Findings	4: 1 High, 2 Medium, 1 Low
Status	Two written replies from the data protection officer (4 and 18 September 2026), three points open on 21 November 2026, no reply to the follow-ups of 17 October and 15 November 2026
SHA-256 (base APK)	`3af9bb84419f7d8fbeef21b6b27cd971eb871e7733ad60d31ef3aeacd2221650`

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 4

4 Architecture & Data Flow 5

5 Engagement Summary 5

6 Findings 6

6.1 H1: The US legal text of the app calls brushing and gum data health data used for advertising and sale, the EU consent text for the same feature never uses the word health . . . 6

6.2 M1: Cleartext HTTP traffic is permitted for the whole app and no certificate is pinned . . . 8

6.3 M2: Firebase API key, Realtime Database URL and Storage bucket of project sonos-mapp are hardcoded in every copy of the app . . . 9

6.4 L1: No technical age verification, the only gate is a self-declared 18 or older Terms clause . . . 10

7 Impact Analysis 10

8 The Complete Chain 11

9 Data Protection: Article by Article 11

10 Consumer Protection & Platform Disclosures 12

11 Regulatory & Legal Landscape 12

12 Indicators of Compromise & Reproducible Evidence 12

13 Disclosure Timeline & Outcome 13

14 What Oral-B Got Right 13

15 Residual Risk & Recommendations 14

Executive Summary

The Oral-B App is the Bluetooth companion app for Oral-B connected toothbrushes. It is published on Google Play under the name P&G Health Care with more than 5 million installs and is rated PEGI 3. On 22 August 2026 RFI-IRFOS disclosed four findings from a root level code analysis of version 10.8.0 under REF ORALB-2026-R1.

This is one of the more carefully built apps in the programme. The manifest holds no pre-consent initialisation of Firebase or any advertising SDK, automatic Firebase and Analytics collection is switched off by default, a granular per-service consent screen exists, a Consumer Health Data Preference Center and a Do Not Sell portal are linked, and the dex payload contains no advertising mediation stack. The findings sit beside that design.

One finding carries the weight. The app's US legal text calls brushing and gum data health data, used among other things for advertising, and states that sensitive personal data may be sold (H1). The EU consent text for the same feature never uses the word health. Two lower findings concern a global cleartext permission (M1) and a hardcoded Firebase key (M2). The person behind H1 is an ordinary user who logs gum bleeding in a toothbrush app and cannot tell from the consent text what category of data that is.

The notice went to the data protection mailbox of Procter & Gamble with the Austrian DSB and the EDPS in copy. The operator's data protection officer answered in writing on 4 September and on 18 September 2026. Both answers were substantive, which is rare in this programme. On 4 and 18 September RFI-IRFOS recorded three points that remain open. Follow-ups of 17 October and 15 November 2026 have had no reply 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 the Google Play release 10.8.0 (versionCode 13821): manifest, resources and dex string pool. The live Google Play listing was read on 2026-08-21 to confirm package, developer and version. No Procter & Gamble server, database or bucket was called, no account was created, no traffic was intercepted and no runtime instrumentation was used. The two operator replies arrived as PDF attachments that could not be read for this report. Their content is taken only from the quotations in the RFI-IRFOS responses of 4 and 18 September 2026 and is marked as recorded.

ID	Severity	Title
H1	HIGH	The US legal text of the app calls brushing and gum data health data used for advertising and sale, the EU consent text for the same feature never uses the word health
M1	MEDIUM	Cleartext HTTP traffic is permitted for the whole app and no certificate is pinned
M2	MEDIUM	Firebase API key, Realtime Database URL and Storage bucket of project sonos-mapp are hardcoded in every copy of the app
L1	LOW	No technical age verification, the only gate is a self-declared 18 or older Terms clause

Finding Status at a Glance

ID	Disclosed	This report	Status on 21 November 2026
H1	HIGH	HIGH	Open. Written operator answer is a no to advertising use. The contradiction with the US text is unresolved.
M1	MEDIUM	MEDIUM	Open. Operator announces an optimisation without date or version. No endpoint list.
M2	MEDIUM	MEDIUM	Open. No answer on the Security Rules.
L1	LOW	LOW	Open. Not addressed in the replies on record.

Subject & Operator Analysis

The app's own legal text names Procter & Gamble Service GmbH, Sulzbacher Str. 40, 65824 Schwalbach am Taunus, Germany, Amtsgericht Königstein im Taunus HRB 6593, as controller for the market Germany, Austria and Switzerland. The global headquarters named in the in-app market imprints is 1 Procter & Gamble Plaza, Cincinnati, OH 45202, USA. The Google Play developer name is P&G Health Care. A related entity at the same address, Procter & Gamble Germany Holding GmbH, HRB 5437, publishes datenschutz.im@pg.com as its data protection contact on its German imprint page. That mailbox is the one that received the notice and the one that answered.

The controller is established in the European Union. For an Austrian initiated matter the Österreichische Datenschutzbehörde can receive a complaint. If the German entity is the main establishment for this processing, the supervisory authority of Hessen could be lead under Article 56 GDPR. That determination is left to the regulators.

No separate Article 27 representative is needed if a Union entity is the controller. The app links a Consumer Health Data Preference Center at preferencecenter.pg.com/en-us/healthdata/, an EU advertising preference page at preferencecenter.pg.com/en-gb/consent-to-advertising/ and a Do Not Sell form at pg-lex.my.salesforce-sites.com/DNSForm/.

Architecture & Data Flow

The app is a native Android application in Kotlin and Java with an embedded Flutter module, five dex files of about 45.5 MB, and the native libraries in a separate install split that was not analysed at binary level. It pairs over Bluetooth with Oral-B iO, Genius and SmartSeries handles and records 16-zone brushing recognition, pressure, a Gum Guard bleeding tracker and week, month and year trend history.

Registration is optional. A guest mode lets a user brush without an account and without cloud sync. Accounts and consent are handled through different legal texts per market, selected by string variants such as _us and _gdpr. The Firebase project behind the app is sonos-mapp. Firebase and Analytics collection are disabled by manifest flags and have to be enabled in code, which the package suggests happens behind the consent screen. The code path was not traced.

Engagement Summary

The notice REF ORALB-2026-R1 was sent on 22 August 2026 at 05:44 UTC to datenschutz.im@pg.com with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It stated H1 with verbatim evidence, summarised M1 and M2 as findings that do not rise above Medium, credited the design of the app, asked three questions and asked for an answer within 14 days.

The data protection officer replied on 4 September 2026 at 13:21 UTC with a statement as a PDF attachment. RFI-IRFOS answered the same day and recorded two points that needed a direct follow-up. A second written reply with a PDF attachment arrived on 18 September 2026 at 08:15 UTC, and RFI-IRFOS recorded the position on the same day. As recorded there, the operator answered both follow-up questions with a no, gave no reasoning for the first and no endpoint list for the second, announced a configuration optimisation for future updates without date or version, and stated that it does not see the relevance of the request under the GDPR and will provide no further information.

A follow-up of 17 October 2026 from security@rfi-irfos.com listed the three open points. No reply is on record. A final notice of 15 November 2026 (11:24 UTC) from security@rfi-irfos.com repeated three questions, named disclosure on 20 November 2026 and asked for an answer by that date. No reply is on record as of 21 November 2026.

Findings

H1: The US legal text of the app calls brushing and gum data health data used for advertising and sale, the EU consent text for the same feature never uses the word health

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 string registration_additional_legal_markdown_us states that by using the app the user consents to the collection of health data, including Product Interests, Individual Health Conditions, Treatments and Diseases, used for the purposes in the P&G Consumer Health Data Privacy Policy, including delivery of relevant advertising. A second string states: NOTICE: We may sell your sensitive personal data. The EU counterpart registration_additional_legal_markdown_gdpr describes the same feature set only as personal data and personalized ads in online media. It never names health data and never mentions Article 9. The Gum Guard bleeding tracker that produces the data has no US-only gate. Its insight text tells every user that gum bleeding could be a sign of gum problems. Operator position as recorded in the correspondence: gum bleeding and brushing data are not used for personalised advertising, not even in the United States. That statement and the US legal text shipped in the same app contradict each other, and neither has been withdrawn or explained. RFI-IRFOS blast-radius escalation: raised from none to HIGH because the app has more than 5 million installs, the data category is a recurring health indicator, and the contradiction sits inside the operator's own shipped legal text. The CVSS vector scores zero because this is a transparency and legal basis finding with no technical attack path.

```
<string name="registration_additional_legal_markdown_us">By using our Oral-B app, you
    consent to the collection of your health data,
including Product Interests, Individual Health Conditions, Treatments and Diseases,
    which will be used for the purposes
outlined in the [P&amp;amp;G Consumer Health Data Privacy Policy](consumerhealthdatalink),
     including delivery of relevant
advertising and management of your account. Your data will be shared with processors
    for legal and operational reasons.
You can withdraw consent through the [Consumer Health Data Preference Center](
    consumerhealthdatapreferencelink).</string>

<string name="legal_notice_may_sell_data_text">NOTICE:  We may sell your sensitive
    personal data.</string>
```

```
<string name="registration_additional_legal_markdown_gdpr">"[Procter &amp; Gamble](
    privacylink), the data controller, will process your
personal data to allow you to register with this app, interact with its services, and,
     depending on your consent,
send you relevant commercial communications, including personalized ads in online
    media. [Find out more](gdprpreferencelink)."</string>

Gum Guard insight text (no _us suffix, no locale gate found):
"You have recorded gum bleeding on high frequency. Gum bleeding could be a sign of gum
     problems. We recommend you visit your dental professional."
```

Gum bleeding history and brushing conditions are plausibly data concerning health under Article 9(1) GDPR, because they reveal a risk indicator for a dental condition. If this data feeds advertising for EU users the way the US text says it does for US users, Article 9(2) requires an exemption that is obtained and labelled separately, most plausibly explicit consent under Article 9(2)(a). A generic personalized ads toggle does not do that. The company wrote precise health data language, a Consumer Health Data Preference Center and a Do Not Sell portal for one jurisdiction, which shows it knows the category. What the package cannot show is whether EU data is used for advertising at all. That is the question the notice put, and the operator has answered it with a written no.

Impact: A user in Austria who logs gum bleeding in the app reads a consent text that speaks of personal data and personalized ads, while the same app tells a user in the United States that this kind of data is health data and may be sold. The EU user has no way to tell from the text which description is true for their own data.

Fix: State in writing and in the EU consent text whether brushing and gum data is used for advertising. If it is not, remove the advertising and sale authorisations from the shipped US text or explain why they are present. If it is, name the data as health data and obtain explicit consent under Article 9(2)(a) in a separate step.

M1: Cleartext HTTP traffic is permitted for the whole app and no certificate is pinned

MEDIUM, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.0 (CVSS-B), disclosed as MEDIUM, open

The network security configuration sets cleartextTrafficPermitted to true in the base-config, with no domain-config that would limit the exception to a single host. Trust anchors are the system store only, so there is no pin-set. With targetSdkVersion 35 the platform default would deny cleartext, so this is a deliberate widening and not an omission. Operator position as recorded in the correspondence: actual traffic with brushing or health data is never sent as cleartext data, and the corresponding optimisation is already planned for future updates. No date and no version number was given, and no list of endpoints that need the exception was provided. Whether any request leaves the app over plain HTTP at runtime was not measured, because no traffic was captured.

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <base-config cleartextTrafficPermitted="true">
        <trust-anchors>
            <certificates src="system" />
        </trust-anchors>
    </base-config>
</network-security-config>
```

```
"niemals als Klartextdaten übertragen"
"die entsprechende Optimierung ist bereits in unseren zukünftigen Updates
    berücksichtigt."
```

Impact: A global cleartext allowance combined with no pinning leaves every connection of the app one mistake away from plain HTTP. A person who logs brushing and gum health on a hostile network would have no protection from the transport layer if a request were ever sent that way. The operator states that this does not happen.

Fix: Remove the global cleartext permission, limit any remaining exception to a named host, add a pin-set for the API hosts the operator controls, and publish the version in which this ships.

M2: Firebase API key, Realtime Database URL and Storage bucket of project sonos-mapp are hardcoded in every copy of the app

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, open

res/values/strings.xml carries the Firebase API key, app ID, project ID, Realtime Database URL, Storage bucket and the Google OAuth web client ID in plain text. Google documents Firebase API keys as not secret by design, so the demonstrated exposure is availability, which means quota exhaustion against the project. The project name sonos-mapp is an internal codename of Oral-B for an iO handle hardware generation, confirmed by resource names such as brush_handle_sonos_galaxy_4 and sonos_firmware_0x6e.bin. It has no relation to the audio company of the same name. Whether the Security Rules of the database and the bucket deny unauthenticated access is not shown by the package, and the live project was not called.

```
<string name="google_api_key">AIzaSyAEYmuq5l36X4T-PppX8T3B4pntTIZ2UXM</string>
<string name="google_crash_reporting_api_key">AIzaSyAEYmuq5l36X4T-PppX8T3B4pntTIZ2UXM
    </string>
<string name="google_app_id">1:360755291208:android:575586f1fecced0f</string>
<string name="project_id">sonos-mapp</string>
<string name="google_storage_bucket">sonos-mapp.appspot.com</string>
<string name="firebase_database_url">https://sonos-mapp.firebaseio.com</string>
<string name="default_web_client_id">360755291208-u01cgujsboduqu5sa6asjeksasecl2mh.
    apps.googleusercontent.com</string>
```

Impact: The key is in every installed copy and cannot be rotated without an app update. If the project were rate limited or billed out, features that depend on it would stop for all users. The burden to show that the database and the bucket deny unauthenticated reads and writes rests with the operator.

Fix: Restrict the key by package name, signing certificate and API scope, enforce App Check for the database and the bucket, and send the Security Rules as evidence.

L1: No technical age verification, the only gate is a self-declared 18 or older Terms clause

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), open

The resource table contains no date of birth field, no age gate screen, no parental consent flow and no under 18 or under 13 string. The only eligibility mechanism is a Terms clause stating that the user is at least 18. The app is rated PEGI 3 on Google Play and the core function, brushing coaching, has no age-sensitive content. A Kids brush head exists as a physical product category in the app. It is not a child account. The marketed children's character feature lives in a separate app, which the package confirms by containing no such string.

```
<string name="account_registration_required_terms_description">You are at least 18,
    have read P&amp;G [Privacy Policy](privacylink)
and agree to the Oral-B Mobile app [Terms of service](termslink).</string>
<string name="registration_legal_text_8_5_markdown">**Terms.** You are at least 18,
    have read P&amp;G [Privacy Policy](privacylink),
and agree to the Oral-B Mobile app [Terms of service](termslink).</string>
```

Impact: A minor could create an account and have gum bleeding history stored without any check. The practical risk is low because the app content is harmless for children and a parent is the likely account holder.

Fix: Document how a parent managing a child's brushing data is expected to use the app, and state the age of eligibility in the consent flow itself.

Impact Analysis

The people affected are users of a toothbrush app with more than 5 million installs, who track brushing and, through Gum Guard, gum bleeding. The data describes a recurring health indicator. The consent they are shown in the EU does not say so.

H1 affects every EU user of Gum Guard and of the profiling consent toggle. M1 affects the transport layer of every connection of the app. M2 concerns the availability of the backend project. L1 affects accounts that a minor might create.

The demonstrated harm is a harm of transparency and configuration. No access to user data was shown and none was attempted. The operator's written position is that EU brushing and gum data is not used for personalised advertising.

The Complete Chain

Step 1, install: a user installs the app from Google Play, which shows PEGI 3 and a Data Safety summary.

Step 2, registration: the user chooses between guest mode and an account. In the EU the registration text speaks of personal data and personalized ads. In the US the same step speaks of health data for advertising and a possible sale (H1).

Step 3, brushing: the app records sessions and, through Gum Guard, gum bleeding. The insight text itself says that gum bleeding could be a sign of gum problems.

Step 4, transport: requests leave the app under a configuration that allows cleartext for every host and pins no certificate (M1). The operator states that no health data travels as cleartext.

Step 5, the user asks what happens with the data: the consent text gives no answer on the health category. The operator's written answer is a no to advertising use, and the contradiction with its own US text remains.

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by H1, because the same feature is described under two different classifications.

Article 6(1) and Article 7(1), lawful basis and conditions for consent: engaged by H1 if EU data feeds advertising.

Article 8, child's consent: touched by L1.

Article 9(1) and Article 9(2), special categories: engaged by H1. Gum bleeding history is plausibly data concerning health. Explicit consent under Article 9(2)(a) would be the likely exemption.

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

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

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

Consumer Protection & Platform Disclosures

The Google Play listing was read on 2026-08-21. It names P&G Health Care as developer, shows more than 5 million installs and rates the app PEGI 3. The rating describes content and says nothing about the processing of health indicators. The text of the Google Play Data Safety section was not read for this report and no statement about it is made.

Regulatory & Legal Landscape

The framework applied is the GDPR, with Article 9 for the classification question in H1 and Article 32 for the configuration findings. The US strings refer to consumer health data laws of individual US states, which explains why the US text uses the term health data. This report makes no assessment under US law.

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.

```
Package            com.pg.oralb.oralbapp
Version            10.8.0 (versionCode 13821), analysed 2026-08-21
base.apk SHA-256   3af9bb84419f7d8fbeef21b6b27cd971eb871e7733ad60d31ef3aeacd2221650
minSdk / targetSdk 30 / 35

Firebase project   sonos-mapp
google_api_key     AIzaSyAEYmuq5l36X4T-PppX8T3B4pntTIZ2UXM
google_app_id      1:360755291208:android:575586f1fecced0f
Storage bucket     sonos-mapp.appspot.com
Database URL       https://sonos-mapp.firebaseio.com
web client id      360755291208-u01cgujsboduqu5sa6asjeksasecl2mh.apps.
    googleusercontent.com
```

```
H1  res/values/strings.xml: registration_additional_legal_markdown_us,
    legal_notice_may_sell_data_text, data_opt_in_description_us,
    registration_additional_legal_markdown_gdpr, register_legal_gdpr,
    gum_bleeding_chart_title, gum_guard_insight_paragraph_professional
M1  res/xml/network_security_config.xml: base-config cleartextTrafficPermitted="true",
     system trust anchors only
M2  res/values/strings.xml: values above
L1  res/values/strings.xml: account_registration_required_terms_description,
    registration_legal_text_8_5_markdown
```

Reproduction: obtain com.pg.oralb.oralbapp 10.8.0 from Google Play, check the SHA-256

above, decode the manifest and resources with apktool and read the named files. No device, account or network access is needed.

Disclosure Timeline & Outcome

2026-08-22 05:44 UTC Notice REF ORALB-2026-R1 to datenschutz.im@pg.com, CC DSB and EDPS. Finding H1 in the text, M1 and M2 summarised, three questions asked, reply requested within 14 days.

2026-09-04 13:21 UTC Written reply from the P&G data protection officer, statement as PDF attachment.

2026-09-04 13:39 UTC RFI-IRFOS response in German, CC DSB and EDPS, recording two points that need a direct follow-up.

2026-09-18 08:15 UTC Second written reply from the data protection officer, PDF attachment.

2026-09-18 10:12 UTC RFI-IRFOS response in German, CC DSB and EDPS, recording the three points that remain open.

2026-10-17 19:31 UTC Follow-up from security@rfi-irfos.com in German, 34 days before the embargo date, listing the three open points. No reply on record.

2026-11-15 11:24 UTC Final notice from security@rfi-irfos.com in German with three questions, announcing disclosure on 20 November 2026. No reply on record.

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

What Oral-B Got Right

No FirebaseInitProvider, no advertising initialisation provider and no other pre-consent tracking provider is declared in the manifest. The dex files contain no advertising mediation SDK, checked for AppLovin, Meta Audience Network, Unity Ads, ironSource, InMobi, Fyber, Moloco, Vungle, Mintegral and Pangle. Firebase Crashlytics, Analytics, advertising ID collection and automatic screen reporting are switched off by manifest flags. A per-service consent screen with a withdrawal path exists. A Consumer Health Data Preference Center and a Do Not Sell portal exist for the US market. allowBackup is true but fullBackupContent is false, which together disable Auto Backup of private data. The dangerous permissions are few and correctly scoped, and BLUETOOTH_SCAN carries neverForLocation. A guest mode avoids forced registration. A named German controller with its own GDPR registration text is shipped in the app. The operator’s data protection officer answered in writing twice.

Residual Risk & Recommendations

Open at the date of publication: three points recorded on 18 September 2026 and repeated on 17 October and 15 November 2026. First, the contradiction between the US legal text and the statement that no advertising use takes place. Second, the global cleartext exception without endpoint list or reasoning. Third, the announced optimisation without date or version. M2 and L1 have not been addressed in the replies on record.

Recommendations: reconcile the US and EU texts so that one description of the data category is true for both, state whether the advertising and sale authorisations in the US text apply to any data of EU users, remove the global cleartext permission and name the version in which this ships, restrict the Firebase key and enforce App Check, and describe the age expectation in the consent flow.

This report is published after the embargo date. Statements are limited to the package and to the public documents named above. The two operator PDFs of 4 and 18 September 2026 were read in full on 21 November 2026 and the summary above matches their text. The operator wrote that data on brushing behaviour and gum bleeding are never used for personalised advertising and that traffic was ”niemals als Klartextdaten übertragen”. It also wrote that ”die entsprechende Optimierung ist bereits in unseren zukünftigen Updates berücksichtigt”. These are statements by the operator, not verified by RFI-IRFOS.

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 Procter & Gamble servers or accounts were probed. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. REF ORALB-2026-R1.