



---

# Sicherheits- & Datenschutz-Offenlegung, Abschlussbericht

## Vignetim Android ([com.vignetim.mobile](https://com.vignetim.mobile))

Eine App für den einmaligen Kauf der österreichischen Autobahn-Jahresvignette um rund 100 Euro enthält Stripe Financial Connections Open-Banking-Kontoverbindung, ein vollständiges Facebook-SDK mit 3.244 Klassen, Mikrofon- und GPS-Präzisionszugriff ohne erkennbaren Zweck, und 71.662 Smali-Klassen für einen einzigen Kaufvorgang, 74 Tage und sechs Nachrichten lang vollständig unbeantwortet, 19 Tage nach Ablauf des Embargos

**ÖFFENTLICHE OFFENLEGUNG, 17. OKTOBER 2026 — EMBARGO ERREICHT AM  
28. SEPTEMBER 2026, FÜNF BEFUNDE UNBEANTWORTET**

---

|                                    |                                                                                                                                                                                                  |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Zielunternehmen</b>             | vignetim.com — privater digitaler Vignetten-Reseller (österreichische Autobahnvignette)                                                                                                          |
| <b>Package</b>                     | com.vignetim.mobile                                                                                                                                                                              |
| <b>Analysierte Plattform</b>       | Android, statische Analyse der Produktions-APK (71.662 Smali-Klassen, React Native)                                                                                                              |
| <b>Erstmeldung (R1)</b>            | 2026-06-30 (REF VIGNETIM-2026-R1-001)                                                                                                                                                            |
| <b>Offenlegungs-/Embargo-Datum</b> | 2026-09-28                                                                                                                                                                                       |
| <b>Bericht veröffentlicht</b>      | 2026-10-17                                                                                                                                                                                       |
| <b>Gesamtschwere</b>               | CRITICAL                                                                                                                                                                                         |
| <b>Befunde</b>                     | 5 (1 Critical, 4 High)                                                                                                                                                                           |
| <b>Korrespondenz</b>               | 6 Nachrichten über 74 Tage an <a href="mailto:privacy@vignetim.com">privacy@vignetim.com</a> und <a href="mailto:info@vignetim.com">info@vignetim.com</a> , 0 Antworten jeder Art, keine Bounces |
| <b>CC Behörden</b>                 | Österreichische Datenschutzbehörde (DSB) · Europäischer Datenschutzbeauftragter (EDPS)                                                                                                           |

---

[security@rfi-irfos.com](mailto:security@rfi-irfos.com) • [rfi-irfos.com](https://rfi-irfos.com)

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

## Contents

---

|           |                                                                                                         |           |
|-----------|---------------------------------------------------------------------------------------------------------|-----------|
| <b>1</b>  | <b>Executive Summary</b>                                                                                | <b>4</b>  |
| <b>2</b>  | <b>Gegenstand &amp; Betreiber-Kontext</b>                                                               | <b>5</b>  |
| <b>3</b>  | <b>Korrespondenz-Zusammenfassung</b>                                                                    | <b>5</b>  |
| <b>4</b>  | <b>Findings</b>                                                                                         | <b>5</b>  |
| 4.1       | C1: 2× Firebase/Google-Maps-API-Keys hartcodiert . . . . .                                              | 5         |
| 4.2       | H1: Stripe Financial Connections: Open-Banking-Bankkontoverbindung auf einer Vignetten-App . . . . .    | 6         |
| 4.3       | H2: Facebook SDK (3.244 Smali-Klassen) auf einer Maut-Kauf-App, Pre-Consent-Init, US-Transfer . . . . . | 6         |
| 4.4       | H3: RECORD_AUDIO + ACCESS_FINE_LOCATION (GPS) ohne erkennbaren Zweck . . . . .                          | 7         |
| 4.5       | H4: Adjust (306 Klassen) + explizite Google-Advertising-ID-Sammlung + 4× BOOT_COMPLETED . . . . .       | 7         |
| <b>5</b>  | <b>Impact-Analyse (Impact Analysis)</b>                                                                 | <b>8</b>  |
| <b>6</b>  | <b>Die vollständige Kette (The Complete Chain): Sechs Nachrichten, 74 Tage, null Antworten</b>          | <b>8</b>  |
| <b>7</b>  | <b>Datenschutz — Artikel für Artikel (Data Protection)</b>                                              | <b>9</b>  |
| <b>8</b>  | <b>Regulatorisches &amp; rechtliches Umfeld (Regulatory)</b>                                            | <b>9</b>  |
| <b>9</b>  | <b>Indicators of Compromise</b>                                                                         | <b>9</b>  |
| <b>10</b> | <b>Offenlegungs-Zeitlinie (Disclosure Timeline) &amp; Ergebnis</b>                                      | <b>10</b> |
| <b>11</b> | <b>Restrisiko &amp; Empfehlungen (Residual Risk)</b>                                                    | <b>10</b> |

## Executive Summary

Vignetim ist eine einfache Kauf-App für die österreichische Autobahn-Jahresvignette (rund 100 Euro), betrieben von vignetim.com, einem privaten digitalen Vignetten-Reseller. Eine Root-Level-Analyse der Produktions-Android-App (com.vignetim.mobile, 71.662 Smali-Klassen, React Native) fand fünf Befunde, einen CRITICAL und vier HIGH — eine Klassenzahl, die für einen einzigen Kaufvorgang architektonisch außergewöhnlich ist.

Zwei Firebase/Google-Maps-API-Keys sind hartcodiert in jeder installierten Kopie (C1). Die App deklariert vier Activities für Stripe Financial Connections, Stripes Open-Banking-Integration für das Verknüpfen und Auslesen von Bankkonten, darunter eine extern aufrufbare (android:exported=true) — eine Funktion, die typischerweise für Bonitätsprüfung oder Direkteinzug eingesetzt wird, nicht für den einmaligen Kauf einer Jahresvignette (H1). Ein vollständiges Facebook-SDK (3.244 Smali-Klassen inkl. AppEvents/Login/Sharing) verknüpft Kaufverhalten mit dem Facebook-Werbenetzwerk und initialisiert via Content-Provider vor jeder Einwilligung (H2). RECORD\_AUDIO und ACCESS\_FINE\_LOCATION sind deklariert, ohne dass für den Kauf einer Autobahnvignette ein Anwendungsfall erkennbar ist, der Mikrofon- oder GPS-Präzisionszugriff erfordert (H3). Adjust (306 Klassen) sowie die explizit aktivierte Google-Advertising-ID-Sammlung und vier BOOT\_COMPLETED-Receiver runden das Bild ab (H4).

RFI-IRFOS meldete diese Befunde am 30. Juni 2026 an [privacy@vignetim.com](mailto:privacy@vignetim.com) und [info@vignetim.com](mailto:info@vignetim.com), CC die österreichische Datenschutzbehörde (DSB) und den EDPS, mit Embargo-Datum 28. September 2026. Über die folgenden 74 Tage sendete RFI-IRFOS fünf weitere Nachrichten. Über sechs Nachrichten insgesamt, ohne einen einzigen Bounce, wurde keine einzige Antwort jeder Art empfangen.

| ID | Severity        | Title                                                                                     |
|----|-----------------|-------------------------------------------------------------------------------------------|
| C1 | <b>CRITICAL</b> | 2× Firebase/Google-Maps-API-Keys hartcodiert                                              |
| H1 | <b>HIGH</b>     | Stripe Financial Connections: Open-Banking-Bankkontoverbindung auf einer Vignetten-App    |
| H2 | <b>HIGH</b>     | Facebook SDK (3.244 Smali-Klassen) auf einer Maut-Kauf-App, Pre-Consent-Init, US-Transfer |
| H3 | <b>HIGH</b>     | RECORD_AUDIO + ACCESS_FINE_LOCATION (GPS) ohne erkennbaren Zweck                          |
| H4 | <b>HIGH</b>     | Adjust (306 Klassen) + explizite Google-Advertising-ID-Sammlung + 4× BOOT_COMPLETED       |

## Gegenstand & Betreiber-Kontext

Vignetim ist kein staatlicher oder ASFINAG-Kanal, sondern ein privater Reseller der österreichischen Autobahnvignette. Die Diskrepanz zwischen dem einfachen, einmaligen Kaufzweck der App und ihrer 71.662-Klassen-Architektur (React Native) mit Open-Banking-, Facebook- und Mikrofon-Integrationen ist der strukturelle Ausgangspunkt dieses Berichts.

## Korrespondenz-Zusammenfassung

RFI-IRFOS sendete die Erstmeldung am 30. Juni 2026 an [privacy@vignetim.com](mailto:privacy@vignetim.com) und [info@vignetim.com](mailto:info@vignetim.com), CC die österreichische Datenschutzbehörde (DSB) und den EDPS, mit Embargo-Datum 28. September 2026 unter REF VIGNETIM-2026-R1-001. Folgenachrichten gingen am 17. Juli, 15. August, 24. August, 31. August und 12. September 2026. Keine der sechs Nachrichten bouncet zu irgendeinem Zeitpunkt; keine wird zu irgendeinem Zeitpunkt beantwortet, auch nicht automatisiert.

## Findings

### C1: 2× Firebase/Google-Maps-API-Keys hartcodiert

**HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 8.1**

```
google_api_key:      [REDACTED IN PUBLIC REPORT -- disclosed privately to Vignetim in R1]
GOOGLE_MAPS_API_KEY: [REDACTED IN PUBLIC REPORT -- disclosed privately to Vignetim in R1]
google_maps_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to Vignetim in R1]
```

**Impact:** RFI-IRFOS blast-radius escalation: von HIGH/8.1 auf CRITICAL angehoben, weil Vignetim eine faktisch verpflichtende Zahlungsapp für eine staatliche Mautgebühr ist, die praktisch jeden Nutzer der österreichischen Autobahnen betreffen kann, nicht ein Nischenprodukt mit kleiner Nutzerbasis. `google_api_key`, `GOOGLE_MAPS_API_KEY` und `google_maps_api_key` sind in `res/values/strings.xml` hartcodiert und in jeder installierten APK-Kopie enthalten. Beide Keys bilden eine Quota-DoS-Angriffsfläche.

## H1: Stripe Financial Connections: Open-Banking-Bankkontoverbindung auf einer Vignetten-App

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 7.6

```
com.stripe.android.financialconnections.FinancialConnectionsSheetActivity
com.stripe.android.financialconnections.FinancialConnectionsSheetNativeActivity
com.stripe.android.financialconnections.lite.FinancialConnectionsSheetLiteActivity
com.stripe.android.financialconnections.lite.
    FinancialConnectionsSheetLiteRedirectActivity
-> android:exported="true" (öffentlich zugänglich)
```

**Impact:** Vier separate Activities für Stripe Financial Connections sind im Manifest deklariert (FinancialConnectionsSheetActivity, FinancialConnectionsSheetNativeActivity und zwei Lite-Varianten), darunter eine mit android:exported=true (extern aufrufbar). Financial Connections ist Stripes Open-Banking-Integration für das direkte Verknüpfen und Auslesen von Bankkonten, typischerweise für Direkteinzug, Kontoverifizierung oder Bonitätsprüfung eingesetzt — nicht für den einmaligen Kauf einer Jahresvignette um rund 96,40 Euro. Der Zweck dieser Integration bleibt in der Datenschutzerklärung undiskutiert.

## H2: Facebook SDK (3.244 Smali-Klassen) auf einer Maut-Kauf-App, Pre-Consent-Init, US-Transfer

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:H/SI:N/SA:N, 7.3

```
3.244 Facebook Smali-Klassen (volle SDK-Integration: AppEvents/Login/Sharing)
com.facebook.internal.FacebookInitProvider -- ContentProvider, Auto-Init vor
    Einwilligung
```

**Impact:** 3.244 Facebook-Smali-Klassen bilden eine vollständige Facebook-SDK-Integration (AppEvents, Login, Sharing) auf einer App, deren einziger Zweck der Kauf einer österreichischen Autobahnvignette ist. Facebook App Events verknüpft Kaufverhalten (Vignettentyp, Kaufzeitpunkt, Gerätedaten) mit dem Facebook-Werbenetzwerk auf Meta Ads-Plattformen. com.facebook.internal.FacebookInitProvider initialisiert via ContentProvider vor dem Einwilligungsbildschirm. Der Kauf einer staatlichen Pflichtgebühr für Mautstraßen ist kein Werbekonversions-Event für Meta; eine Rechtsgrundlage für die Übermittlung dieser Kauf-Event-Daten an Meta (USA) ist nicht erkennbar.

### H3: RECORD\_AUDIO + ACCESS\_FINE\_LOCATION (GPS) ohne erkennbaren Zweck

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 7.0

```
<uses-permission android:name="android.permission.RECORD_AUDIO"/>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
```

**Impact:** android.permission.RECORD\_AUDIO ist deklariert; für den Kauf einer Autobahnvignette ist kein Anwendungsfall erkennbar, der Mikrofonzugriff erfordert. android.permission.ACCESS\_FINE\_LOCATION (GPS-Präzisionsstandort) ist ebenfalls deklariert; sofern die App einen grenznahen Vignette-Reminder-Service anbietet, wäre dies mit ACCESS\_COARSE\_LOCATION (Netzwerkstandort) datensparend umsetzbar — GPS-Präzision für einen Grenzübertritt-Reminder übersteigt die Erforderlichkeit nach Art. 5(1)(c).

### H4: Adjust (306 Klassen) + explizite Google-Advertising-ID-Sammlung + 4x BOOT\_COMPLETED

HIGH, 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, 7.2

```
com.adjust.sdk.AdjustReferrerReceiver (android:exported="true") -- 306 Klassen
google_analytics_adid_collection_enabled: true
ReactNativeFirebaseAppInitProvider (initOrder=99) -- vor Einwilligung
4x BOOT_COMPLETED Receiver
```

**Impact:** com.adjust.sdk.AdjustReferrerReceiver (android:exported=true, 306 Klassen) misst Attribution für bezahlte Werbekampagnen. google\_analytics\_adid\_collection\_enabled ist explizit auf true gesetzt und aktiviert damit ausdrücklich die Sammlung der Google Advertising ID. ReactNativeFirebaseAppInitProvider initialisiert mit initOrder=99, vor Einwilligung. Vier BOOT\_COMPLETED-Receiver starten mehrere Komponenten bereits beim System-Boot, ohne dass der Nutzer die App geöffnet hat.

## Impact-Analyse (Impact Analysis)

---

C1 ist eine standardmäßige Credential-Exposition, hier als CRITICAL eingestuft, weil Vignetim eine faktisch verpflichtende Zahlungsapp für eine staatliche Mautgebühr ist und damit praktisch jeden Autobahnnutzer in Österreich betreffen kann. H1 ist der konzeptionell ungewöhnlichste Befund dieses Berichts: eine Open-Banking-Integration auf einer App, deren einziger Geschäftszweck ein einmaliger Kauf um rund 100 Euro ist, lässt sich mit diesem Zweck allein nicht erklären. H2 bis H4 zeigen zusammen ein durchgängiges Muster: ein einfaches Kaufprodukt trägt die vollständige Tracking- und Attribution-Infrastruktur einer Werbe-finanzierten Consumer-App, inklusive Berechtigungen (Mikrofon, GPS-Präzision), für die innerhalb des eigentlichen Produktzwecks kein Anwendungsfall erkennbar ist.

Sechs Nachrichten über 74 Tage, an zwei funktionierende, nie gebouncete Adressen, produzierten keine einzige Antwort jeder Art.

### Die vollständige Kette (The Complete Chain): Sechs Nachrichten, 74 Tage, null Antworten

---

Schritt 1 — Meldung gesendet: RFI-IRFOS sendet den vollständigen Befundbericht am 30. Juni 2026 an [privacy@vignetim.com](mailto:privacy@vignetim.com) und [info@vignetim.com](mailto:info@vignetim.com), CC die österreichische DSB und den EDPS, mit Embargo-Datum 28. September 2026.

Schritt 2 bis 5 — Vier Folgenachrichten, identisches Ergebnis: RFI-IRFOS sendet weitere Nachrichten am 17. Juli, 15. August, 24. August und 31. August 2026, jede mit den drei wiederholten Fragen und den verstrichenen Tagen. Kein Bounce wird je verzeichnet, keine automatische Bestätigung, keine menschliche Antwort.

Schritt 6 — Letzte Folgenachricht: Am 12. September 2026, 74 Tage nach der Erstmeldung, stellt RFI-IRFOS fest, dass über fünf vorherige Nachrichten keine Antwort jeder Art empfangen wurde. Auch diese Nachricht bleibt unbeantwortet.

Schritt 7 — Embargo erreicht und überschritten: Das am 30. Juni 2026 einmalig genannte Embargo-Datum verstreicht am 28. September 2026, alle fünf Befunde unbeantwortet.

Schritt 8 — Veröffentlichung: Dieser Bericht erscheint 19 Tage nach dem Embargo-Datum. Über 109 Tage und sechs Nachrichten an zwei durchgehend funktionierende Adressen enthält die Korrespondenz null Antworten jeder Art.

## Datenschutz — Artikel für Artikel (Data Protection)

---

Art. 32(1)(b) DSGVO — Sicherheit der Verarbeitung: C1s hartcodierte Keys ohne erkennbare Schutzmaßnahme.

Art. 5(1)(b), Art. 13, Art. 6(1) DSGVO — Zweckbindung, Transparenz, Rechtsgrundlage: H1s Open-Banking-Integration hat keinen erkennbaren Bezug zum deklarierten App-Zweck und keine ausgewiesene Rechtsgrundlage.

Art. 5(1)(b), Art. 6(1), Art. 44-49, Art. 7 DSGVO — Zweckbindung, Rechtsgrundlage, Drittlandtransfer, Einwilligung: H2s Facebook-Integration verknüpft einen Pflichtgebühren-Kauf mit Werbekonversion ohne erkennbare Rechtsgrundlage und initialisiert vor Einwilligung.

Art. 5(1)(c), Art. 13 DSGVO — Datenminimierung, Transparenz: H3s Mikrofon- und GPS-Präzisionszugriff übersteigen die Erforderlichkeit für den deklarierten Zweck.

Art. 7 DSGVO — Bedingungen für die Einwilligung: H4s Adjust-Attribution und Advertising-ID-Sammlung sind ohne erkennbaren Bezug zur Einwilligung aktiv.

## Regulatorisches & rechtliches Umfeld (Regulatory)

---

Vignetim ist ein privater digitaler Reseller der österreichischen Autobahnvignette, kein staatlicher ASFINAG-Kanal. Die österreichische Datenschutzbehörde (DSB) und der Europäische Datenschutzbeauftragte (EDPS) wurden über die ursprüngliche Meldung und jede Folgenachricht informiert (DSGVO Art. 83(2)(b)).

Bußgeldrahmen nach DSGVO: Art. 83(4) ist auf alle fünf Befunde anwendbar, bis zu 10.000.000 € oder 2 % des weltweiten Jahresumsatzes. Dass ein Anbieter einer faktisch verpflichtenden Zahlungsapp für eine staatliche Mautgebühr auf sechs schriftliche Meldungen über 74 Tage nicht reagiert, auch nicht automatisiert, ist ein Faktum, das eine Aufsichtsbehörde neben den fünf technischen Befunden mit abwägen dürfte.

## Indicators of Compromise

---

Die folgenden Identifikatoren, SDK-Pakete und Manifest-Deklarationen wurden ausschließlich durch statische Analyse der Produktions-APK extrahiert. Es wurden keine Vignetim-, Stripe-, Facebook- oder Adjust-Server, -Konten oder -Infrastruktur geprüft.

```
C1 -- google_api_key, GOOGLE_MAPS_API_KEY: [REDACTED IN PUBLIC REPORT -- disclosed
    privately to Vignetim in R1]

H1 -- com.stripe.android.financialconnections.* (4 Activities, 1 exported=true)

H2 -- 3.244 Facebook-Klassen, com.facebook.internal.FacebookInitProvider

H3 -- android.permission.RECORD_AUDIO, android.permission.ACCESS_FINE_LOCATION

H4 -- com.adjust.sdk.AdjustReferrerReceiver (306 Klassen),
    google_analytics_adid_collection_enabled=true
```

## Offenlegungs-Zeitlinie (Disclosure Timeline) & Ergebnis

---

2026-06-30 Erstmeldung an [privacy@vignetim.com](mailto:privacy@vignetim.com) und [info@vignetim.com](mailto:info@vignetim.com), CC österreichische DSB, EDPS. Embargo: 2026-09-28. REF VIGNETIM-2026-R1-001.

2026-07-17, 2026-08-15, 2026-08-24, 2026-08-31 Vier Folgenachrichten. Kein Bounce, keine automatische Bestätigung, keine menschliche Antwort, an keinem Punkt.

2026-09-12 Letzte Folgenachricht, 74 Tage seit der Erstmeldung. Keine Antwort folgt.

2026-09-28 Embargo-Datum erreicht, wie am 2026-06-30 einmalig genannt und nie revidiert. Korrespondenz-Stand: sechs RFI-IRFOS-Nachrichten, null Antworten jeder Art, keine Bounces.

2026-10-17 Dieser Bericht veröffentlicht, 19 Tage nach dem Embargo-Datum.

## Restrisiko & Empfehlungen (Residual Risk)

---

C1 — Sofort: hartcodierte Firebase- und Google-Maps-Keys rotieren und aus dem Quellcode in eine sichere Secrets-Verwaltung verschieben.

H1 — Sofort: entweder die Stripe-Financial-Connections-Integration entfernen, falls sie nicht dem deklarierten Kaufzweck dient, oder ihren konkreten Geschäftszweck und ihre Rechtsgrundlage transparent in der Datenschutzerklärung ausweisen, und die exportierte Activity auf `android:exported=false` setzen, sofern kein externer Aufruf benötigt wird.

H2 — Kurzfristig: FacebookInitProvider hinter die Einwilligungsentscheidung legen und den Geschäftszweck der Verknüpfung eines Mautgebühren-Kaufs mit Werbekonversion dokumentieren oder die Integration entfernen.

H3 — Kurzfristig: RECORD\_AUDIO entfernen, sofern ungenutzt; ACCESS\_FINE\_LOCATION durch ACCESS\_COARSE\_LOCATION ersetzen, sofern der Zweck ein grenznaher Reminder-Service ist.

H4 — Kurzfristig: ReactNativeFirebaseAppInitProvider hinter die Einwilligungsentscheidung legen, `google_analytics_adid_collection_enabled` auf die tatsächliche Einwilligungslogik koppeln.

Alle Befunde — einen überwachten Intake-Pfad für Sicherheits- und Datenschutzmeldungen an [privacy@vignetim.com](mailto:privacy@vignetim.com) und [info@vignetim.com](mailto:info@vignetim.com) einrichten: sechs schriftliche Meldungen über 74 Tage ohne jede Antwort sind ein eigenständiger Prozessfehler.

---

**RFI-IRFOS** [security@rfi-irfos.com](mailto:security@rfi-irfos.com) • [rfi-irfos.com](https://rfi-irfos.com)

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria Alle Befunde beruhen auf statischer Analyse der

veröffentlichten Anwendung mittels öffentlich verfügbarer Werkzeuge. Es wurden keine Vignetim-, Stripe-, Facebook- oder Adjust-Server, -Konten oder -Infrastruktur geprüft. Technische Nachweise sind unter Chain of Custody archiviert und werden Aufsichtsbehörden auf Anfrage zur Verfügung gestellt. Forschung durchgeführt gemäß ISO/IEC 29147, der Freiheit der Wissenschaft (Art. 17 StGG) und DSGVO Art. 89. REF VIGNETIM-2026-R1-001.