



Security & Privacy Disclosure, Final Report

Mein Magenta for Android (at.tmobile.android.myt)

A genuinely engaged DPO answered five technical findings in detail across two written replies, and then the one finding her own words had surfaced, an undisclosed Indian sub-processor named as a joint controller, went unanswered through two direct follow-ups and a 21-day-overdue embargo

PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 26 SEPTEMBER 2026, ONE FINDING REMAINS UNRESOLVED

Target	Magenta Telekom (T-Mobile Austria GmbH), subsidiary of Deutsche Telekom AG (XETRA: DTE)
Package	at.tmobile.android.myt
Platform Audited	Android · v26.2609.31 (versionCode 66329), static analysis of the production APK
Initial Disclosure (R1)	2026-06-26 (REF MAGENTA-MYT-2026)
Disclosure / Embargo Date	2026-09-26
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	6 (1 Critical, 1 High, 3 Medium, 1 Low, 5 of 6 substantively addressed by the operator)
Correspondence	10 messages sent by RFI-IRFOS, 2 detailed written technical replies received from Magenta's DPO (27 July and 17 August 2026), 1 offer of a phone call declined in favour of written correspondence, 0 replies after 1 September 2026
Authorities BCC'd / CC'd	Austrian Datenschutzbehörde (DSB) · RTR (Rundfunk und Telekom Regulierungs-GmbH)

security@rfi-irfos.com • rfi-irfos.com

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

Contents

1	Executive Summary	4
2	Subject & Operator Context	5
3	Engagement Summary	6
4	Findings	6
4.1	C1: CleverTap and its operating partner, Nuclei CDNA Technologies Private Limited (India), are absent from Magenta's own published processor list despite Magenta's own description of Nuclei as a joint controller	7
4.2	H1: No confirmed GDPR Art. 35 data protection impact assessment for the app's combined processing activities	8
4.3	M1: Cobrowse.io dual InitProvider initializes on every app launch, ahead of any consent screen, though Magenta's reply credibly limits actual data transmission to an explicit, customer-initiated session	8
4.4	M2: Three Google API keys hardcoded in the production binary, with Magenta stating server-side key restrictions as the mitigating control	9
4.5	M3: Huawei HMS AAID InitProvider auto-initializes with the highest priority observed in this audit round, with Magenta citing a dual Play Store/AppGallery distribution model and a graceful fallback on non-Huawei devices	10
4.6	L1: BOOT_COMPLETED, precise location, READ_PHONE_STATE and CALL_PHONE permissions, each with a specific stated purpose	10
5	Impact Analysis	11
6	The Complete Chain: A Careful Answer That Revealed the Gap It Never Closed	11
7	Data Protection — Article by Article	12
8	Regulatory & Legal Landscape	13
9	Indicators of Compromise	13
10	Disclosure Timeline & Outcome	14
11	Residual Risk & Recommendations	15

Executive Summary

Magenta Telekom (T-Mobile Austria GmbH), a subsidiary of Deutsche Telekom AG, operates Mein Magenta, the primary account-management Android application for its telecom customers, used to view bills, call history, data usage, and payment methods. Static analysis of v26.2609.31 identified six findings, ranging from a live screen co-browsing SDK that initializes on every app launch to an undisclosed Indian sub-processor revealed by Magenta's own written reply.

This case differs from most others in this disclosure series: Magenta's Datenschutzbeauftragte, Dr. Natalie Ségur-Cabanac, engaged substantively in writing on two separate occasions, on 27 July 2026 addressing the Cobrowse.io and CleverTap/MoEngage findings in detail, and on 17 August 2026 addressing the hardcoded API keys, the Huawei advertising component, and the device-permission findings, each with specific, plausible technical detail rather than a generic denial. RFI-IRFOS credits this engagement directly in this report rather than treating it identically to the silent or self-contradicting cases elsewhere in this series: the Cobrowse.io screen-sharing SDK, while it does initialize on every app launch, only transmits data after a customer explicitly starts a session and shares a one-time code; the hardcoded API keys are, by Magenta's account, restricted server-side to the app's own certificate signature; the Huawei advertising component fails gracefully on non-Huawei devices; and the device permissions each carry a specific, stated purpose.

What Magenta's own 27 July 2026 reply also did, in the course of explaining its CleverTap integration, was surface a finding RFI-IRFOS had not originally identified: CleverTap is used by Magenta's partner Nuclei to operate 'Magenta Moments', a voucher-redemption feature, and Magenta's own reply describes Nuclei CDNA Technologies Private Limited, based in Bangalore, India, as a joint controller under Art. 26 GDPR for these transactions. Magenta's own published list of data processors names Cobrowse.io (via Sprinklr) and MoEngage correctly, but does not name CleverTap or Nuclei at all. RFI-IRFOS raised this gap, and a related question about whether a GDPR Art. 35 impact assessment exists for the app's combination of processing activities, on 18 August 2026. Magenta's DPO replied the same day offering a phone call rather than continuing in writing; RFI-IRFOS declined, consistent with this disclosure programme's written-only correspondence policy, and restated the open questions on 24 August and, in expanded six-question form, on 1 September 2026. No reply of any kind followed either message. The stated embargo of 26 September 2026 passed 21 days before this report's publication date with that one finding, raised by Magenta's own words, still unaddressed.

ID	Severity	Title
C1	CRITICAL	CleverTap and its operating partner, Nuclei CDNA Technologies Private Limited (India), are absent from Magenta's own published processor list despite Magenta's own description of Nuclei as a joint controller
H1	HIGH	No confirmed GDPR Art. 35 data protection impact assessment for the app's combined processing activities
M1	MEDIUM	Cobrowse.io dual InitProvider initializes on every app launch, ahead of any consent screen, though Magenta's reply credibly limits actual data transmission to an explicit, customer-initiated session

ID	Severity	Title
M2	MEDIUM	Three Google API keys hardcoded in the production binary, with Magenta stating server-side key restrictions as the mitigating control
M3	MEDIUM	Huawei HMS AAID InitProvider auto-initializes with the highest priority observed in this audit round, with Magenta citing a dual Play Store/AppGallery distribution model and a graceful fallback on non-Huawei devices
L1	LOW	BOOT_COMPLETED, precise location, READ_PHONE_STATE and CALL_PHONE permissions, each with a specific stated purpose

Subject & Operator Context

Magenta Telekom (T-Mobile Austria GmbH) is one of Austria's three major mobile network operators and a subsidiary of Deutsche Telekom AG, listed on the XETRA exchange. Mein Magenta, its Android account-management app (at.tmobile.android.myt), is the primary digital channel through which customers view bills, data usage, call history, contract terms, and payment methods, and manage eSIM provisioning.

As a telecommunications provider, Magenta is subject to Austria's Telekommunikationsgesetz 2021 (TKG 2021), including its confidentiality-of-communications provisions under Section 165, in addition to GDPR. The findings in this report concern an app that displays exactly the kind of billing, usage, and contact data that confidentiality-of-communications law is written to protect, alongside a live screen-sharing SDK, device-location and identifier permissions, and a third-party voucher integration that, by the operator's own description, involves a joint controller in India.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 26 June 2026 to datenschutz@magenta.at and security@magenta.at (the latter bounced, and bounced again on a 6 July 2026 follow-up), CC.presse@magenta.at and kundenservice@magenta.at, BCC the Austrian DSB and RTR.

Magenta's DPO, Dr. Natalie Ségur-Cabanac, acknowledged on 8 July 2026 that the findings had been forwarded to Magenta's technical experts. After a follow-up on 23 July 2026, she replied substantively on 27 July 2026, addressing the Cobrowse.io screen-sharing architecture and the CleverTap/MoEngage analytics integration in specific technical detail, including a description of Nuclei CDNA Technologies Private Limited (India) as a joint controller for a voucher-redemption feature. RFI-IRFOS confirmed in its 27 July reply that two of five original findings had been substantively addressed and three remained open.

After two further follow-ups (4 and 9 August 2026), Magenta's DPO replied again on 17 August 2026, addressing the three remaining original findings, the hardcoded API keys, the Huawei advertising component, and the device permissions, each with specific stated justifications and mitigations. Her message closed by stating she considered all questions answered and further correspondence unnecessary.

RFI-IRFOS replied the same day, 18 August 2026, confirming that B2, B3, and B5 had indeed been addressed, while raising a GDPR Art. 35 impact-assessment question that remained open and a new finding, triggered directly by Magenta's own 27 July description of Nuclei's role: Nuclei and CleverTap are both absent from Magenta's own published processor list. Magenta's DPO replied the same day offering a phone call rather than continuing by email; RFI-IRFOS declined in writing, consistent with this programme's written-only correspondence policy, and restated the open points. Two further follow-ups, 24 August and 1 September 2026 (the latter posing six specific questions on the processor-list gap, the India transfer, and the Art. 35 question), received no reply of any kind. The stated embargo of 26 September 2026 passed 21 days before this report's publication date.

Findings

C1: CleverTap and its operating partner, Nuclei CDNA Technologies Private Limited (India), are absent from Magenta's own published processor list despite Magenta's own description of Nuclei as a joint controller

CRITICAL (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, 5.3) — undisclosed third-country joint controller, confirmed by the operator's own written reply, blast-radius escalated from MEDIUM

"Nuclei fuehrt zusaetzlich anonymisierte Analysen von Kaufverhalten...
Magenta und Nuclei agieren hier als gemeinsame Verantwortliche
gemaess Artikel 26 DSGVO... Fuer die Abwicklung der Kaeufe von
Gutscheinkarten arbeitet Magenta Telekom mit Nuclei CDNA
Technologies Private Limited (Bangalore, Karnataka, Indien)
als Partner zusammen."

Magenta's published processor list (magenta.at/unternehmen/dienstleister) names Cobrowse.io and MoEngage. CleverTap and Nuclei CDNA Technologies are not present on that list.

Impact: RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.3 to CRITICAL because this finding is not an inference, it is confirmed by Magenta's own 27 July 2026 written reply, which describes Nuclei CDNA Technologies Private Limited (Bangalore, India) as a joint controller under Art. 26 GDPR for Magenta Moments voucher transactions, processing purchase-behaviour data via the CleverTap SDK embedded in the app. Magenta's own published processor list names Cobrowse.io (via Sprinklr) and MoEngage, demonstrating the list is actively maintained, yet omits both CleverTap and Nuclei. No Art. 46 transfer safeguard for the resulting transfer to India was identified in any reply. RFI-IRFOS raised this directly on 18 August 2026 and restated it with six specific questions on 1 September 2026; neither received any reply before the embargo date.

H1: No confirmed GDPR Art. 35 data protection impact assessment for the app's combined processing activities

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, 4.0) — unanswered accountability question on a multi-SDK telecom app, blast-radius escalated from MEDIUM

"Liegt eine dokumentierte DSFA nach Art. 35 DSGVO fuer Mein Magenta vor, insbesondere fuer die Kombination aus Screensharing-Infrastruktur, Geofencing und zwei Engagement-Plattformen. Ja oder nein, bei Ja das Datum der Erstellung." -- sent 2026-08-18, restated 2026-09-01, no reply received to either message.

Impact: RFI-IRFOS blast-radius escalation: raised from MEDIUM/4.0 to HIGH because this is not a hypothetical process question, it concerns a telecom app combining a live screen-sharing SDK, GPS geofencing, device-identifier access, and two parallel engagement/analytics platforms (CleverTap, MoEngage) on billing and usage data for a TKG 2021-regulated provider's customer base. RFI-IRFOS asked this question directly on 18 August and again on 1 September 2026; Magenta's final written reply (17 August) did not address it, and no later reply, written or otherwise, ever did.

M1: Cobrowse.io dual InitProvider initializes on every app launch, ahead of any consent screen, though Magenta's reply credibly limits actual data transmission to an explicit, customer-initiated session

MEDIUM (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 2.4) — pre-consent SDK readiness, materially mitigated by the operator's documented consent-gated session model

```
<provider android:name="io.cobrowse.CobrowseInitProvider" .../>
<provider android:name="io.cobrowse.CobrowseComposeInitProvider" .../>
```

Magenta's stated mitigation: session requires explicit customer-initiated start plus a session-specific code shared with the support agent; no video recording; sensitive fields (passwords, payment details) automatically redacted from agent view.

Impact: Magenta's 27 July 2026 reply, with a published privacy-policy citation, states that Cobrowse.io's auto-initializing ContentProviders only prepare the SDK for a possible screen-sharing session, that no data is transmitted at this stage, and that an actual session requires the customer to actively start it and share a session-specific code with a support agent before any screen access is granted, consistent with Art. 6(1)(a) consent captured via an in-app confirmation button. RFI-IRFOS has not independently verified the network behaviour of the auto-initializing provider beyond Magenta's written account. The residual finding is narrower than originally scoped: the SDK's infrastructure is network-ready before consent,

even though data transmission itself is credibly gated behind an explicit, session-specific user action.

M2: Three Google API keys hardcoded in the production binary, with Magenta stating server-side key restrictions as the mitigating control

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, 2.3) — hardcoded credentials, mitigated by stated but unverified server-side restrictions

```
google_api_key (Firebase), awareness_api_key (Google Awareness),  
geofence_api_key (same as awareness), geo_api_key (Geo/Maps)  
project_id: one-app-austria
```

Magenta's stated mitigation: SHA-1/SHA-256 certificate-fingerprint restriction, Firebase Security Rules, quota/rate limiting, continuous access monitoring.

Impact: Magenta's 17 August 2026 reply states the three hardcoded keys (Firebase, Google Awareness/Geofencing, Geo/Maps, project one-app-austria) are restricted server-side to the app's registered certificate signature, governed by Firebase Security Rules, subject to quota and rate limiting, and continuously monitored for anomalous access patterns. RFI-IRFOS has not independently verified these server-side controls, which is a standard limitation of a static, client-side audit rather than a reason to doubt the claim. Hardcoding client-restricted API keys in a production binary remains a finding worth recording as a matter of defense-in-depth, but the credible, specific mitigation described materially reduces the residual risk from the CRITICAL rating this class of finding has carried elsewhere in this disclosure series where no such explanation was offered.

M3: Huawei HMS AAID InitProvider auto-initializes with the highest priority observed in this audit round, with Magenta citing a dual Play Store/AppGallery distribution model and a graceful fallback on non-Huawei devices

MEDIUM (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 3.1) — pre-consent initialization with a stated functional purpose and no-op fallback

```
<provider android:name="com.huawei.hms.aid.InitProvider"
  android:initOrder="500" .../>
```

Magenta's stated mitigation: dual Play Store / Huawei AppGallery distribution; graceful no-op fallback on non-Huawei devices; split-APK separation under review.

Impact: Magenta's 17 August 2026 reply states the Huawei HMS AAID InitProvider exists because Mein Magenta ships as a single package to both the Google Play Store and the Huawei AppGallery, to serve customers on Huawei devices without Google Mobile Services, and that on non-Huawei devices the provider detects the absence of Huawei system services and generates no advertising identifier and transmits no data, a stated 'graceful fallback'. Magenta also stated it is reviewing a split-APK architecture to separate the Huawei-specific component entirely. RFI-IRFOS has not independently re-verified the fallback behaviour on a non-Huawei device for this report. The initOrder=500 priority, the highest observed in this audit round, remains a pre-consent initialization regardless of the fallback claim, which is why this finding is retained rather than closed, but the specific, plausible functional justification offered materially reduces its severity relative to an unexplained pre-consent tracker.

L1: BOOT_COMPLETED, precise location, READ_PHONE_STATE and CALL_PHONE permissions, each with a specific stated purpose

LOW (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 1.8) — device permissions with specific, plausible stated purposes and explicit runtime consent for location

```
RECEIVE_BOOT_COMPLETED -- push/notification renewal after reboot
ACCESS_FINE_LOCATION   -- shop-finder, runtime-consent gated
READ_PHONE_STATE       -- SIM/eSIM detection, network status
CALL_PHONE/CALL_COMPANION -- user-initiated tap-to-call support
```

Impact: Magenta's 17 August 2026 reply assigns each permission a specific purpose: RECEIVE_BOOT_COMPLETED for push-registration renewal and scheduled billing/usage notifications after reboot; ACCESS_FINE_LOCATION for a shop-finder feature only, gated behind the Android runtime permission dialog with no location access absent explicit grant; READ_PHONE_STATE for SIM/eSIM detection and network-status display rather than IMEI-based profiling; CALL_PHONE/CALL_COMPANION for a user-initiated tap-to-call customer-service feature; and geofencing for shop-proximity notifications, also gated behind the location permission. These are specific, functionally plausible justifications rather than a blanket

assertion, and this finding is recorded as LOW on that basis, down from the HIGH severity this permission combination has carried in other cases in this series where no comparable explanation was given.

Impact Analysis

This report differs in shape from most others in this disclosure series because Magenta's DPO engaged substantively, in writing, on two separate occasions, with specific technical detail rather than a generic acknowledgment or a self-contradicting denial. M1 through L1 reflect that engagement directly: each finding's severity was reduced from where it would otherwise sit, because Magenta provided a specific, plausible, and in most cases independently checkable justification that RFI-IRFOS has no evidence to dispute.

C1 and H1 are different in kind. C1 is not a finding RFI-IRFOS inferred from the binary; it is a finding Magenta's own written reply surfaced, while attempting to explain something else. A joint controller in India, processing voucher-purchase behaviour data, absent from the operator's own published processor list, is exactly the kind of transparency gap GDPR Art. 13 and Art. 26 exist to prevent, and it carries Art. 44/46 third-country transfer obligations that no reply ever addressed. H1, the absence of a confirmed Art. 35 impact assessment for the app's full combination of processing activities, was asked twice and answered neither time. The operator that handled five findings carefully left exactly these two unaddressed, and did so after indicating, on 18 August, that it considered the correspondence closed.

The Complete Chain: A Careful Answer That Revealed the Gap It Never Closed

Step 1 — Disclosure: RFI-IRFOS sends five findings (B1-B5) to datenschutz@magenta.at on 26 June 2026.

Step 2 — Acknowledgment and forwarding: Magenta's DPO confirms on 8 July 2026 that the findings were forwarded to technical experts.

Step 3 — First substantive reply: On 27 July 2026, the DPO addresses Cobrowse.io (B1) and CleverTap/MoEngage (B4) in detail, including a description of Nuclei CDNA Technologies Private Limited (India) as a joint controller under Art. 26 GDPR, a fact not previously known to RFI-IRFOS.

Step 4 — A new finding surfaces from the operator's own words: RFI-IRFOS checks Magenta's published processor list against this description and finds Nuclei and CleverTap both absent, despite the list correctly naming Cobrowse.io and MoEngage.

Step 5 — Second substantive reply: On 17 August 2026, the DPO addresses the hardcoded API keys (B2), the Huawei component (B3), and the device permissions (B5), each with specific justification, and states she considers the correspondence complete.

Step 6 — The gap is raised directly: RFI-IRFOS replies the same day, confirming B2/B3/B5 as addressed, and raising the processor-list gap and the open Art. 35 question for the first time as a named, specific point.

Step 7 — An offer to move off the record: The DPO replies the same day, stating email is no longer productive and offering a phone call. RFI-IRFOS declines in writing, consistent with this programme's written-only policy, which exists precisely so that a disclosure's record stays reviewable by regulators and the public rather than depending on an unrecorded conversation.

Step 8 — Silence: Two further follow-ups, 24 August and 1 September 2026, the second posing six specific written questions about the India transfer and the Art. 35 question, receive no reply of any kind.

Step 9 — Publication: The embargo of 26 September 2026 passes, and this report publishes 21 days later, with five of six findings resolved by the operator's own careful engagement, and the sixth, the one that engagement itself revealed, still open.

Data Protection — Article by Article

Art. 13(1)(e) GDPR — Transparency, recipients of data: C1's absence of CleverTap and Nuclei from Magenta's own published processor list, despite Magenta naming Cobrowse.io and MoEngage correctly on the same list.

Art. 26 GDPR — Joint controllers: C1 concerns a relationship Magenta itself describes as a joint-controller arrangement with Nuclei under Art. 26, without the corresponding Art. 26(2) transparency obligation (naming the arrangement to data subjects) appearing to have been met via the processor list.

Art. 44/Art. 46 GDPR — Transfers to third countries: C1's transfer of purchase-behaviour data to Nuclei in India has no stated Art. 46 safeguard identified in any reply received.

Art. 35 GDPR — Data protection impact assessment: H1's question, whether a DPIA exists for the combination of screen-sharing, geofencing, and dual engagement-platform processing, was asked twice and never answered.

Art. 7(1) GDPR — Conditions for consent: M1's Cobrowse.io and M3's Huawei AAID components both initialize before any consent screen, materially mitigated in both cases by stated, specific limits on what data actually moves before a further user action.

Art. 32 GDPR — Security of processing: M2's hardcoded API keys, materially mitigated by Magenta's stated server-side key restrictions and Firebase Security Rules.

Art. 5(1)(c) GDPR — Data minimisation: L1's device permissions, each assigned a specific stated purpose by Magenta's own reply.

Regulatory & Legal Landscape

Magenta Telekom is an Austrian TKG 2021-regulated telecommunications provider and a subsidiary of Deutsche Telekom AG (XETRA: DTE). The Austrian Datenschutzbehörde (DSB) and RTR, the Austrian telecommunications regulator, were BCC'd from the original disclosure and CC'd on subsequent follow-ups.

Fine exposure under GDPR: Art. 83(5) applies to the Art. 26 joint-controller transparency gap and the unaddressed Art. 44/46 transfer question in C1, up to EUR 20,000,000 or 4% of total worldwide annual turnover, calculated at the Deutsche Telekom group level given Magenta's subsidiary status. Art. 83(4) applies to the Art. 35, 7, 5, and 32 matters in H1 and M1-L1, up to EUR 10,000,000 or 2% of total worldwide annual turnover. Section 165 TKG 2021, Austria's telecommunications confidentiality provision, is independently relevant to any of the location, device-identifier, or usage-data processing touched on in this report, though RFI-IRFOS found Magenta's stated purposes for that processing specific and plausible rather than clearly non-compliant.

Indicators of Compromise

The following identifiers and permission declarations were extracted from the production APK (v26.2609.31) via static analysis only. No Magenta servers, accounts, or infrastructure were probed. Several findings in this report were clarified or substantially mitigated by Magenta's own written replies, cited and quoted where directly relevant above.

```
C1 -- CleverTap SDK, operated by Nuclei CDNA Technologies Private
    Limited (Bangalore, India); absent from Magenta's published
    processor list (magenta.at/unternehmen/dienstleister)

M1 -- io.cobrowse.CobrowseInitProvider, CobrowseComposeInitProvider

M2 -- 3 hardcoded Google API keys, project: one-app-austria

M3 -- com.huawei.hms.aaid.InitProvider, initOrder=500

L1 -- android.permission.RECEIVE_BOOT_COMPLETED,
    ACCESS_FINE_LOCATION, READ_PHONE_STATE, CALL_PHONE
```

Disclosure Timeline & Outcome

2026-06-26 Initial disclosure sent to datenschutz@magenta.at and security@magenta.at (bounced). CC: presse@magenta.at, kundenservice@magenta.at. BCC: Austrian DSB, RTR.

2026-07-06 Follow-up, security@magenta.at bounces again.

2026-07-08 Magenta's DPO acknowledges, confirms findings forwarded to technical experts.

2026-07-23/24 Follow-up; DPO asks for a named point of contact, RFI-IRFOS responds with its already-public team identity.

2026-07-27 Magenta's DPO sends a detailed written reply addressing B1 (Cobrowse.io) and B4 (CleverTap/MoEngage), surfacing the Nuclei CDNA Technologies (India) joint-controller relationship.

2026-08-04, 2026-08-09 Follow-ups on the three remaining findings.

2026-08-17 Magenta's DPO sends a second detailed written reply addressing B2 (API keys), B3 (Huawei AAID), and B5 (device permissions), stating she considers the matter closed.

2026-08-18 RFI-IRFOS confirms B2/B3/B5 addressed, raises the processor-list gap (new finding, now C1) and the open Art. 35 question (H1). Magenta's DPO offers a phone call in place of further written correspondence; RFI-IRFOS declines in writing.

2026-08-24 Follow-up, CC Austrian DSB. No reply.

2026-09-01 Final follow-up, six specific questions on the India transfer, the processor list, and the Art. 35 question. No reply.

2026-09-26 Stated embargo date reached. No further message of any kind received from Magenta since the 18 August phone-call offer.

2026-10-17 This report published, 21 days after the embargo date. Five of six findings resolved or substantially mitigated by Magenta's own written engagement; C1 and H1 remain open on the correspondence record.

Residual Risk & Recommendations

C1 — Immediate: Add CleverTap and Nuclei CDNA Technologies Private Limited to the published processor list, consistent with the Art. 26 joint-controller relationship Magenta's own reply already describes, and document the Art. 46 transfer mechanism relied on for the resulting transfer to India.

H1 — Immediate: Confirm in writing whether a GDPR Art. 35 impact assessment exists for Mein Magenta's combined processing (screen-sharing, geofencing, dual engagement platforms), and if not, commission one given the scale of the TKG 2021-regulated customer base involved.

M1 — Governance: Consider gating Cobrowse.io's ContentProvider initialization itself behind a lighter-weight flag rather than full SDK init, to remove even the pre-consent network-readiness window, given the stated session-gated data model already in place.

M2 — Governance: Continue the stated key-restriction and monitoring controls; consider migrating to a server-mediated token exchange to remove hardcoded keys from the client entirely as a defense-in-depth improvement.

M3 — Governance: Complete the stated split-APK review to remove the Huawei AAID component from the non-Huawei distribution entirely, removing the pre-consent initialization question rather than relying on the graceful-fallback behaviour.

Across all findings: this case demonstrates that a specific, evidenced written reply measurably changes how a finding is scored in this disclosure series. RFI-IRFOS encourages Magenta to close the one gap its own engagement surfaced with the same specificity it brought to the other five.

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 All findings derive from static root-level analysis of

the published application using publicly available tooling. Several findings were clarified or materially mitigated by direct written correspondence with Magenta's Datenschutzbeauftragte, quoted where directly relevant. No Magenta servers, accounts, or infrastructure were probed. Technical evidence is archived under chain of custody and will be provided to regulatory authorities on request. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF MAGENTA-MYT-2026.