



Sicherheits- & Datenschutz-Offenlegung, Abschlussbericht

Magenta SmartHome (de.telekom.smarthomeb2c)

Marketing- und Attributions-Stack (MoEngage, Adjust, Usabilla) trotz selbst gehosteter Telemetrie, globaler Klartext-Verkehr in einer App mit Kamera- und Schlossdaten; von Telekom nur automatische Bestätigungen, die Landesdatenschutzbehörde NRW verneinte ihre Zuständigkeit

**ÖFFENTLICHE OFFENLEGUNG, 17. OKTOBER 2026, EMBARGO ERREICHT AM 29.
SEPTEMBER 2026, KEINE INHALTLICHE ANTWORT DES UNTERNEHMENS,
AUFSICHT VERNEINT ZUSTÄNDIGKEIT**

Zielunternehmen	Deutsche Telekom AG, Bonn (QIVICON-Plattform); die LDI NRW nennt als Hersteller die Telekom Deutschland GmbH
Package	de.telekom.smarthomeb2c, Version 6.8.1 (versionCode 381)
Analysierte Plattform	Android, statische Analyse der Produktions-APK (134 MB, einzelne APK)
Erstmeldung (R1)	2026-07-01 (REF MAGENTA-2026-R1-001)
Embargo-Datum	2026-09-29
Bericht veröffentlicht	2026-10-17
Gesamtschwere	HIGH
Befunde	6 (2 High, 3 Medium, 1 Low)
Korrespondenz	8 Sendungen von RFI-IRFOS (2026-07-01 bis 2026-09-18), 2 automatische Eingangsbestätigungen von Telekom (01.07., 17.07.), keine inhaltliche Antwort des Unternehmens; LDI NRW: automatische Bestätigung am 2026-08-17 und inhaltliche Antwort von Herrn Dr. Meis am 2026-09-17; kein Bounce
CC Behörden	DSB Österreich · EDPS · LDI NRW (ab 2026-08-15)
SHA-256 (base APK)	2a8d64260b1b73584294f3d710eacdc542198713732087e44e85246cb1e8f9cf

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	Gegenstand & Betreiber-Kontext	5
3	Korrespondenz-Zusammenfassung	5
4	Was korrekt umgesetzt ist (Honest Positives)	5
5	Findings	6
5.1	H1: Marketing-Stack (MoEngage, Adjust, Usabilla) trotz Self-Hosting, MoEngage-Region nicht bestimmbar	6
5.2	H2: Network Security Config erlaubt Klartext global, kein Pinning	6
5.3	M1: Adjust-Auto-Init und AD_ID vor dem Einwilligungs-Wizard möglich	7
5.4	M2: Google-/Firebase-API-Schlüssel im Klartext	7
5.5	M3: Breiter Berechtigungssatz für eine Heimsteuerung	7
5.6	L1: Eingebetteter Sentry-DSN (selbst gehostet) und US-Feedback-SDK	8
6	Impact-Analyse (Impact Analysis)	8
7	Die vollständige Kette (The Complete Chain)	8
8	Datenschutz, Artikel für Artikel (Data Protection)	8
9	Regulatorisches & rechtliches Umfeld (Regulatory)	9
10	Indicators of Compromise	9
11	Offenlegungs-Zeitlinie (Disclosure Timeline) & Ergebnis	10
12	Restrisiko & Empfehlungen (Residual Risk)	11

Executive Summary

Magenta SmartHome ist die Whole-Home-Steuerung der Deutschen Telekom auf der eigenen QIVICON-Cloud. Eine Root-Level-Analyse der Produktions-APK (Version 6.8.1) fand sechs Befunde: zwei HIGH, drei MEDIUM, einen LOW. Es gibt keinen CRITICAL-Befund.

Die App ist in ihrem Kern deutlich sauberer als vergleichbare Apps chinesischer Hersteller: Authentifizierung, Backend und Sprache laufen über Telekom-eigene EU-Infrastruktur, Produktanalyse (Countly) und Absturzberichte (Sentry) sind selbst gehostet, Firebase Analytics ist abgeschaltet.

Genau deshalb fällt der aufgesetzte externe Marketing-Layer auf (H1): MoEngage, Adjust (mit Werbe-ID, Auto-Init) und Usabilla (Momentive, USA) in einer App, die Kamera-Streams, Türschlösser, Fensterkontakte und Anwesenheit verarbeitet. Die Datenregion von MoEngage ist aus der Binärdatei nicht bestimmbar, eine US-Übermittlung nicht auszuschließen. H2: Die Network Security Config erlaubt Klartext-Verkehr global ohne Pinning.

Von der Telekom selbst kam in 110 Tagen keine inhaltliche Antwort, nur zwei automatische Eingangsbestätigungen. Die LDI NRW bestätigte den Eingang automatisch und erklärte am 17. September, Hersteller seien keine Normadressaten der DSGVO und verwies auf das BSI. RFI-IRFOS widersprach am 18. September mit dem Argument, dass Telekom hier den Dienst Ende-zu-Ende selbst betreibt. Darauf liegt keine Antwort vor.

ID	Severity	Title
H1	HIGH	Marketing-Stack (MoEngage, Adjust, Usabilla) trotz Self-Hosting, MoEngage-Region nicht bestimmbar
H2	HIGH	Network Security Config erlaubt Klartext global, kein Pinning
M1	MEDIUM	Adjust-Auto-Init und AD_ID vor dem Einwilligungs-Wizard möglich
M2	MEDIUM	Google-/Firebase-API-Schlüssel im Klartext
M3	MEDIUM	Breiter Berechtigungssatz für eine Heimsteuerung
L1	LOW	Eingebetteter Sentry-DSN (selbst gehostet) und US-Feedback-SDK

Gegenstand & Betreiber-Kontext

Magenta SmartHome (Magenta Zuhause) ist ein Dienst der Deutschen Telekom auf der QIVICON-Plattform (Region de99). Authentifizierung über Telekom IDM, Backend unter qivi-con.com, Sprachsteuerung über das Magenta Voice Kit. Die App verarbeitet Kamera- und RTSP-Streams, Schlossstatus, Fensterkontakte, Thermostate und Anwesenheit per Hintergrundstandort.

Die Datenschutzerklärung ist in der App über einen Einwilligungs-Wizard (DataPrivacyActivity) eingebunden. Eine Datenschutzbeauftragten-Adresse steht nicht in der Binärdatei.

Korrespondenz-Zusammenfassung

Die Erstmeldung ging am 1. Juli 2026 an datenschutz@telekom.de, mit DSB, EDPS und der LDI NRW in BCC (der Originalversand hatte kein sichtbares Regulator-CC), Embargo 29. September. Es folgten Nachfassungen am 6. Juli, 17. Juli, 27. Juli, 15. August, 31. August und 11. September, alle mit denselben drei Fragen. Telekom schickte zwei automatische Eingangsbestätigungen (1. und 17. Juli) und keine inhaltliche Antwort.

Ab 15. August stand die LDI NRW im CC. Ihre Poststelle bestätigte am 17. August automatisch. Am 17. September antwortete Herr Dr. Meis (Referat 23, Az. 23.64.2026-0016486): Hersteller seien nach der DSGVO keine Normadressaten, Verantwortliche seien die Kunden; Art. 25 DSGVO binde Hersteller nicht, Erwägungsgrund 78 enthalte nur einen Appell. Er empfahl, sich an das BSI zu wenden.

RFI-IRFOS antwortete am 18. September (Telekom, DSB, EDPS und LDI Poststelle im CC): Bei Magenta SmartHome betreibe Telekom den Dienst Ende-zu-Ende selbst (eigene IDM, eigene QIVICON-Cloud, Vertragskunden für genau diesen Dienst, Entscheidung über die eingebundenen SDKs) und sei damit Verantwortliche nach Art. 4 Nr. 7 DSGVO. Die Empfehlung zum BSI wurde angenommen. Auf diese Präzisierung liegt zum Berichtsdatum keine Antwort vor.

Was korrekt umgesetzt ist (Honest Positives)

- Selbst gehostete Produktanalyse (County) und Absturzberichte (Sentry) auf der eigenen deutschen QIVICON-Cloud, auf dem Niveau eines Sauberkeits-Benchmarks.
- Firebase bewusst gezügelt: firebase_analytics_collection_enabled=false, firebase_messaging_auto_init_enabled=false, Sentry-Auto-Init aus.
- Keine chinesischen oder sanktionierten SDKs, keine .cn-, aliynucs- oder myqcloud-Endpunkte, kein aktives Ad-Serving.
- Einwilligungs-Wizard, GdprForgetMe und OptOut-Funktionen vorhanden.
- allowBackup=false, nicht debuggable, targetSdk 36, EU-Infrastruktur für Authentifizierung, Backend und Sprache.

Findings

H1: Marketing-Stack (MoEngage, Adjust, Usabilla) trotz Self-Hosting, MoEngage-Region nicht bestimmbar

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, 7.5

```
com/moengage/* (807+124), sdk-01..04.moengage.com, DATA_CENTER_1..6
com/adjust/* (309+1), app.adjust.com, SystemLifecycleContentProvider, AD_ID
com/usabilla/* (1565+30), api.usabilla.com
Selbst gehostet: countly-prod.cloud.qivicon.com, sentry.monitoring.magentazuhausa.app
```

Region und Init-Zeitpunkt vor dem Einwilligungs-Wizard sind laufzeitabhängig und wurden nicht gemessen.

Impact: Eine Smart-Home-App mit Kamera-, Schloss-, Fenster- und Anwesenheitsdaten bindet drei externe Anbieter ein: MoEngage (Marketing-Automation, Datenzentren DC1 bis DC6 gebündelt), Adjust (Attribution mit Werbe-ID, Auto-Init-ContentProvider) und Usabilla (Momentive, USA). Da Telekom Telemetrie nachweislich selbst hosten kann, ist die Notwendigkeit dieser Verarbeiter nicht selbsterklärend (Art. 5(1)(c)). Die konfigurierte MoEngage-Region liegt in obfuskiertem Code.

H2: Network Security Config erlaubt Klartext global, kein Pinning

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, 7.5

```
<network-security-config>
  <base-config cleartextTrafficPermitted="true" />
</network-security-config>
```

Impact: Die Datei network_security_config.xml setzt base-config cleartextTrafficPermitted=true ohne domain-config und ohne pin-set. Bei targetSdk 36 ist Klartext standardmäßig verboten; die App aktiviert ihn anwendungsweit wieder und pinnt kein Zertifikat, in einer App, die Kamera-Streams, Schlossstatus und Anwesenheit transportiert. Ob ein Endpunkt tatsächlich per HTTP erreicht wird, ist laufzeitabhängig.

M1: Adjust-Auto-Init und AD_ID vor dem Einwilligungs-Wizard möglich

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.3

Architektur bestätigt, Zeitpunkt nicht gemessen.

Impact: Der Adjust-ContentProvider läuft beim Prozessstart, AD_ID und Install-Referrer sind deklariert. GDPR-Hilfen (GdprForgetMe, OptOut, withConsent) sind vorhanden, die Reihenfolge gegenüber dem Wizard ist laufzeitabhängig.

M2: Google-/Firebase-API-Schlüssel im Klartext

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.3

```
google_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to
  Deutsche Telekom in R1]
google_crash_reporting_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to
  Deutsche Telekom in R1]
google_maps_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to
  Deutsche Telekom in R1]
firebase_database_url: [REDACTED IN PUBLIC REPORT -- disclosed privately to
  Deutsche Telekom in R1]
```

Impact: Zwei Schlüssel (Firebase/Crash Reporting und Maps) samt Projektkoordinaten sind aus strings.xml extrahierbar. Ohne serverseitige Restriktionen drohen Quota- und Abrechnungsgerschöpfung.

M3: Breiter Berechtigungssatz für eine Heimsteuerung

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.3

Ob eine DSFA vorliegt, wurde dreimal gefragt und nicht beantwortet.

Impact: Hintergrundstandort mit Geofencing (ComingHome), Kamera, Mikrophon (Voice Kit), Kontakte, Telefonstatus und Bluetooth. Jede Berechtigung hat eine plausible Funktion; die Kombination erfüllt regelmäßig die Schwelle für eine Datenschutz-Folgenabschätzung nach Art. 35. Governance-Befund, kein Überwachungsvorwurf.

L1: Eingebetteter Sentry-DSN (selbst gehostet) und US-Feedback-SDK

LOW, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3

Der DSN ist im öffentlichen Bericht nicht wiedergegeben.

Impact: Ein selbst gehosteter Sentry-DSN ist im Binary (ingest-only, geringes Risiko, Self-Hosting positiv). Offen bleibt die US-Verarbeitung durch Usabilla (siehe H1).

Impact-Analyse (Impact Analysis)

H1 und H2 treffen die sensibelste Datenkategorie dieses Falls: Kamera, Schloss und Anwesenheit im Haushalt. Der Kern der App ist sauber gebaut, was beide Befunde umso auffälliger macht.

Die vollständige Kette (The Complete Chain)

Schritt 1: Erstmeldung 1. Juli 2026 an datenschutz@telekom.de, automatische Bestätigung.

Schritt 2: Fünf Nachfassungen bis 11. September, drei Fragen wortgleich wiederholt, ab 15. August LDI NRW im CC; zweite automatische Bestätigung am 17. Juli.

Schritt 3: Inhaltliche Antwort der LDI NRW am 17. September (Zuständigkeit verneint, BSI-Hinweis). Antwort von RFI-IRFOS am 18. September, bis heute unbeantwortet.

Schritt 4: Embargo am 29. September erreicht, Veröffentlichung 18 Tage danach, 108 Tage nach der Erstmeldung. Von der Telekom liegt keine inhaltliche Antwort vor.

Datenschutz, Artikel für Artikel (Data Protection)

Art. 5(1)(c), 6(1), 7 DSGVO: Notwendigkeit und Rechtsgrundlage der externen SDKs (H1, M1).

Art. 44, 46 DSGVO: MoEngage-Region und Usabilla in den USA (H1).

Art. 32, 5(1)(f) DSGVO: globaler Klartext, API-Schlüssel (H2, M2).

Art. 35 DSGVO: DSFA für Standort, Kamera, Schloss und Sprache (M3).

Regulatorisches & rechtliches Umfeld (Regulatory)

Die Verantwortlichkeit der Deutschen Telekom AG für den selbst betriebenen Dienst ist nach Auffassung von RFI-IRFOS gegeben (Art. 4 Nr. 7 DSGVO). Die LDI NRW vertrat am 17. September die Gegenposition, Hersteller seien keine Normadressaten, und nannte die Telekom Deutschland GmbH als Hersteller. Die Frage, ob bei einem Ende-zu-Ende selbst betriebenen Dienst die Herstellerausnahme greift, ist nicht entschieden und wird hier unverändert dokumentiert.

Der Hinweis auf das BSI (§ 5 BSIG, Coordinated Vulnerability Disclosure) wurde angenommen. DSB und EDPS stehen in Kenntnis.

Indicators of Compromise

Technische Fundstellen der Produktions-APK. Schlüssel und Tokens sind im öffentlichen Bericht redigiert.

```
Package: de.telekom.smarthomeb2c 6.8.1 (381)
SHA-256: 2a8d64260b1b73584294f3d710eacdc542198713732087e44e85246cb1e8f9cf
Firebase: [REDACTED IN PUBLIC REPORT -- disclosed privately to Deutsche Telekom in R1]
Selbst gehostet: countly-prod.cloud.qivicon.com, sentry.monitoring.magentazuhause.app
Extern: sdk-01..04.moengage.com, app.adjust.com, api.usabilla.com
NSC: base-config cleartextTrafficPermitted=true
```

Datum	Ereignis
-------	----------

Offenlegungs-Zeitlinie (Disclosure Timeline) & Ergebnis

Datum	Ereignis
2026-07-01	Erstmeldung an datenschutz@telekom.de; automatische Bestätigung
2026-07-06	Nachfassung 1, keine Antwort
2026-07-17	Nachfassung 2; zweite automatische Bestätigung
2026-07-27	Nachfassung 3, Fragen wortgleich
2026-08-15	Nachfassung 4 (DSB, EDPS, LDI NRW im CC)
2026-08-17	Automatische Bestätigung der LDI-Poststelle
2026-08-31	Nachfassung 5
2026-09-11	Nachfassung 6
2026-09-17	Inhaltliche Antwort LDI NRW (Dr. Meis): Zuständigkeit verneint, Hinweis BSI
2026-09-18	Antwort RFI-IRFOS zur Verantwortliche Eigenschaft, unbeantwortet
2026-09-29	Embargo erreicht
2026-10-17	Veröffentlichung dieses Berichts

Korrespondenzbilanz: acht Sendungen von RFI-IRFOS, zwei automatische Bestätigungen der Telekom, keine inhaltliche Antwort des Unternehmens, eine inhaltliche Antwort der Aufsichtsbehörde (Zuständigkeit verneint), kein Bounce. Der Fall wird mit diesem Bericht geschlossen. Eine nachträgliche Antwort von Telekom oder der Aufsicht wird neben den Befunden vermerkt.

Restrisiko & Empfehlungen (Residual Risk)

Alle Befunde sind zum Berichtsdatum nicht als behoben dokumentiert. Die Rechtsfrage zur Verantwortlichkeit bleibt zwischen RFI-IRFOS und der LDI NRW offen. Der Bericht beruht auf statischer Analyse. Laufzeitverhalten (Zeitpunkt der ersten Netzwerkaufrufe, serverseitige Schlüsselrestriktionen, Datenregion) wurde nicht gemessen und ist als solches gekennzeichnet. Die Betreiber können diese Punkte jederzeit durch Dokumentation belegen oder widerlegen.

- MoEngage-Datenzentrum und Garantien (SCC, TIA) für MoEngage und Usabilla dokumentieren; Notwendigkeit gegenüber der vorhandenen Eigen-Infrastruktur begründen.
 - Adjust und MoEngage erst nach Einwilligung initialisieren (Auto-Init-Provider deaktivieren).
 - Network Security Config auf Domain-Scope mit Pinning umstellen, Klartext abschalten.
 - Google-Schlüssel per Paket und Signatur beschränken; DSFA nach Art. 35 für die Kombination aus Standort, Kamera, Schloss und Sprache erstellen.
-

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 Alle Befunde beruhen auf statischer Analyse der veröffentlichten Anwendung mittels öffentlich verfügbarer Werkzeuge. Es wurden keine Server, Konten oder Infrastruktur des Betreibers 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 MAGENTA-2026-R1-001.