



Coordinated Security & Privacy Disclosure, Final Report

ViCare, ViGuide and ViParts for Android

Three apps, one exchange: confirmed within two days, reported to the supervisory authority by the vendor itself, fixed and independently verified

PUBLIC DISCLOSURE, 26 OCTOBER 2026 – REMEDIATION VERIFIED

Target	Viessmann Holding International GmbH, Allendorf (Eder), Germany. A Carrier company (Carrier Global Corporation, NYSE: CARR)
Products audited	ViCare (com.viessmann.vicare), ViGuide (com.viessmann.vizard.presentation.release), ViParts (com.viessmann.viparts), all for Android
Disclosure references	REF VC-2026-R1-001, VG-2026-R1-001, VP-2026-R1-001
First notice	2026-06-30 (ViCare), 2026-07-02 (ViGuide, ViParts)
Disclosure / embargo date	2026-09-28 (ViCare), 2026-09-30 (ViGuide, ViParts)
Re-verification	2026-10-26, current Play Store builds pulled from an RFI-IRFOS test device
Report published	2026-10-26
Lead supervisory authority	Hessischer Beauftragter für Datenschutz und Informationsfreiheit (HBDI), notified by Viessmann on 2 July and 28 July 2026
Outcome	REMEDIATION VERIFIED. All critical findings fixed or rotated. Two minor ViGuide items announced as fixed are still in the binary

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 Analysis	6
3	Re-verification Method, 26 October 2026	6
4	Status Overview	7
5	Positive Observations	7
6	Findings	7
6.1	VC-C2: ViCare: Firebase initialised before consent. VERIFIED FIXED	8
6.2	VC-C1: ViCare: Firebase API key in the APK. UNCHANGED, restriction not verifiable	9
6.3	VC-H1: ViCare: background location and boot-time geofencing. ACCEPTED	9
6.4	VC-H2: ViCare: cleartext permitted in the base network config. ACCEPTED	9
6.5	VC-H3: ViCare: privacy policy does not name every Firebase subsystem. PARTIALLY ADDRESSED	10
6.6	VG-C1: ViGuide: Firebase API key in the APK. VERIFIED FIXED (rotated)	10
6.7	VG-C2: ViGuide: Firebase and ML Kit initialised before consent. VERIFIED FIXED	10
6.8	VG-H1: ViGuide: app-wide cleartext traffic. VERIFIED FIXED	11
6.9	VG-H2: ViGuide: KPIT diagnostics host still referenced. OPEN, dormant	11
6.10	VG-H3: ViGuide: data of installation owners processed by a B2B app. ADDRESSED BY STATEMENT	11
6.11	VG-M1: ViGuide: password field in a generated toString(). OPEN	12
6.12	VG-M2: ViGuide: internal hosts in the production binary. PARTIALLY FIXED	12
6.13	VG-L1: ViGuide: advertising ID permission and Bluetooth scope. UNCHANGED, assessed by Viessmann	12
6.14	VP-C1: ViParts: Firebase keys in the APK. FIXED for the native key, web key unchanged	13
6.15	VP-H1: ViParts: Firebase bootstrap before consent. VERIFIED FIXED for Analytics	13
6.16	VP-M1: ViParts: API gateway key in client JavaScript. VERIFIED FIXED	13
6.17	VP-M2: ViParts: staging and integration URLs in production. UNCHANGED	14
6.18	VP-M3: ViParts: allowBackup enabled. UNCHANGED	14
6.19	VP-L1: ViParts: AD_ID permission and custom-scheme OAuth callback. UNCHANGED	14
7	Impact Analysis	14
8	The Complete Chain	15
9	Data Protection, Article by Article	15
10	Regulatory Framework	16
11	Indicators of Compromise	16
12	Disclosure Timeline	17
13	Residual Risk & Recommendations	18

Executive Summary

Between 30 June and 2 July 2026, RFI-IRFOS notified Viessmann of security and data protection findings in three Android apps. ViCare is the consumer app that controls Viessmann heating systems and heat pumps in private homes. ViGuide is the commissioning and service app used by heating technicians. ViParts is the spare-parts catalogue for trade partners.

Viessmann's response is the best RFI-IRFOS has received in the 2026 research programme. The Head of Data Protection answered within two days, point by point, confirmed the central ViCare finding with technical detail, and reported it to the Hessian supervisory authority (HBDI) on 2 July 2026, before RFI-IRFOS asked for anything. The ViGuide and ViParts findings followed to HBDI on 28 July. Fixes shipped on 29 July (ViCare 3.39.1), 3 August (ViParts 1.10.2) and 12 August 2026 (ViGuide 2.24.9).

On 26 October 2026, RFI-IRFOS pulled the current Play Store builds (ViCare 3.41.3, ViGuide 2.24.13, ViParts 1.11.4) and checked every finding against them. The pre-consent Firebase start is fixed in all three apps through the Usercentrics CMP and Consent Mode v2. The ViGuide Firebase key and the ViParts native key were rotated. App-wide cleartext in ViGuide is gone. The ViParts API gateway key has been removed from the JavaScript bundle. The ViGuide Jira URLs are gone.

Two ViGuide items that Viessmann listed as addressed on 3 September are still present in v2.24.13: the reference to the KPIT diagnostics host and a generated toString() that prints the gateway password field. Both are minor. Neither shows a reachable data flow. They are documented here because the record has to match the binary. The remaining items are hygiene findings that Viessmann placed in its regular release process, and RFI-IRFOS agrees with that classification.

World context, queried on 26 October 2026 from the DINGIR feed, CISA KEV and NVD (14-day window): no known exploited vulnerability and no new CVE concerns the Viessmann apps or their stack. The keyword hits for Carrier and KPIT were name collisions with unrelated products.

Scope: Static analysis of the production Android APKs of ViCare, ViGuide and ViParts, installed from Google Play on an RFI-IRFOS test device. June 2026 for the notices, 26 October 2026 for the re-verification. Manifest, resources, dex strings and bundled JavaScript. No live backend testing, no credential use, no traffic interception.

Disposition

Viessmann answered the first notice within two days, confirmed the central finding, notified HBDI on 2 July and 28 July 2026, and shipped fixes for all three apps between 29 July and 12 August 2026. RFI-IRFOS verified the fixes against the current Play Store builds on 26 October 2026. Two minor ViGuide items remain in the binary.

ID	Severity	Title
VC-C2	MEDIUM	ViCare: Firebase initialised before consent. VERIFIED FIXED
VC-C1	MEDIUM	ViCare: Firebase API key in the APK. UNCHANGED, restriction not verifiable
VC-H1	LOW	ViCare: background location and boot-time geofencing. ACCEPTED
VC-H2	LOW	ViCare: cleartext permitted in the base network config. ACCEPTED
VC-H3	LOW	ViCare: privacy policy does not name every Firebase subsystem. PARTIALLY ADDRESSED
VG-C1	MEDIUM	ViGuide: Firebase API key in the APK. VERIFIED FIXED (rotated)
VG-C2	MEDIUM	ViGuide: Firebase and ML Kit initialised before consent. VERIFIED FIXED
VG-H1	MEDIUM	ViGuide: app-wide cleartext traffic. VERIFIED FIXED
VG-H2	LOW	ViGuide: KPIT diagnostics host still referenced. OPEN, dormant
VG-H3	LOW	ViGuide: data of installation owners processed by a B2B app. ADDRESSED BY STATEMENT
VG-M1	LOW	ViGuide: password field in a generated toString(). OPEN
VG-M2	LOW	ViGuide: internal hosts in the production binary. PARTIALLY FIXED
VG-L1	LOW	ViGuide: advertising ID permission and Bluetooth scope. UNCHANGED, assessed by Viessmann
VP-C1	MEDIUM	ViParts: Firebase keys in the APK. FIXED for the native key, web key unchanged
VP-H1	MEDIUM	ViParts: Firebase bootstrap before consent. VERIFIED FIXED for Analytics
VP-M1	MEDIUM	ViParts: API gateway key in client JavaScript. VERIFIED FIXED
VP-M2	LOW	ViParts: staging and integration URLs in production. UNCHANGED
VP-M3	LOW	ViParts: allowBackup enabled. UNCHANGED
VP-L1	LOW	ViParts: AD_ID permission and custom-scheme OAuth callback. UNCHANGED

Subject & Operator Analysis

Viessmann Holding International GmbH, Viessmannstraße 1, 35108 Allendorf (Eder), registered at Amtsgericht Marburg, HRB 3861. Since January 2024 Viessmann Climate Solutions belongs to Carrier Global Corporation (NYSE: CARR). The data protection contact for all three apps is Carrier's Head of Data Protection for Viessmann, who handled the whole exchange. The lead supervisory authority is the Hessian Commissioner for Data Protection and Freedom of Information (HBDI).

App	Users	Role	Data processed
ViCare	Private households	Remote control of heating, heat pumps, photovoltaics and storage	Account, heating and energy data, presence through geofencing, installation location
ViGuide	Heating technicians	Commissioning, diagnosis and remote service of installations	Technician account, installation data of third-party owners, gateway credentials
ViParts	Trade partners	Spare-parts catalogue and ordering	Business account, order and search data

A heating system app knows when people are at home. Heating curves, heat pump runtimes and geofence events together form a presence profile of a household. That is the reason RFI-IRFOS rated the pre-consent finding in ViCare as the central item in June.

Re-verification Method, 26 October 2026

RFI-IRFOS installed the current builds from Google Play on a test device (vivo V2247) and pulled the base APK and every split over ADB. Each file was compared by SHA-256 against the on-device hash. The manifest and resources were decoded with apktool. The dex files and bundled JavaScript assets were searched for every string named in the June notices. No live backend call was made, and no credential was used.

App	Version (code)	SHA-256 base APK
ViCare	3.41.3 (20000545)	0f51af609d16a71b7002b30fb01f4cd 2a45c3525ea6493450061778a648f 3e6b
ViGuide	2.24.13 (2040001158)	c1df1b7f14c119324b3506a6687a4f2 a212c68ee1873fbef41e0a6b783bf0 279
ViParts	1.11.4 (71)	357bfa3254f1c771bde2c9a13ca04d 386c0d47bc7e3256fb149f697393b 5ffdb

Limitation: one ViGuide feature split carrying ODX diagnostic data could not be pulled because the USB connection dropped repeatedly. None of the findings concerns that split. Every check ran on the base APK, which carries the manifest, the dex code and the resources.

Status Overview

App	Verified fixed	Accepted / addressed by statement	Open
ViCare	C2 pre-consent start	H1 geofencing, H2 local cleartext, H3 partially	C1 key restriction not verifiable
ViGuide	C1 key rotated, C2 pre-consent, H1 cleartext, M2 Jira URLs	H3 owner transparency, L1	H2 KPIT reference, M1 password toString, M2 two hosts
ViParts	C1 native key rotated, H1 Analytics, M1 gateway key	L1	C1 web key restriction, M2 staging URLs, M3 allowBackup

Positive Observations

Viessmann did everything a coordinated disclosure asks of a vendor, and did it early. It answered within two days. It confirmed the finding in its own words rather than disputing the wording. It reported to its supervisory authority on its own initiative, twice. It fixed the consumer app first, then carried the same fix into the two business apps without being asked. It gave version numbers and rollout dates that RFI-IRFOS could check, and they checked out.

ViCare sets allowBackup=false. None of the three apps ships a Chinese SDK or a biometric identity SDK. All three now route Analytics through one CMP, which makes consent auditable in one place.

Findings

VC-C2: ViCare: Firebase initialised before consent. VERIFIED FIXED**MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 5.1**

June 2026 (v3.39.0): FirebaseInitProvider was declared directBootAware with initOrder 100 and started Firebase Analytics before any consent dialog could be shown. Viessmann confirmed the finding on 2 July 2026, reported it to the Hessian supervisory authority (HBDI) the same day, and shipped Consent Mode v2 with processing denied by default in v3.39.1 on 29 July 2026. Status on 26 October 2026 (v3.41.3): fixed in substance.

v3.41.3, 26 Oct 2026

Usercentrics CMP:	present (1,712 SDK strings in classes*.dex)
Consent Mode v2 at runtime:	setConsent / ConsentType / analytics_storage present
FirebaseInitProvider:	still directBootAware="true", initOrder="100"
Manifest consent defaults:	none (google_analytics_default_allow_* absent)

The consent decision now governs Analytics through the Usercentrics CMP and Consent Mode v2 at runtime. That is the fix Viessmann described, and the binary carries it. One narrow residue remains. FirebaseInitProvider still starts first, and the manifest declares no default of "denied". The window between process start and the first setConsent call therefore depends on code order inside the app. Static analysis cannot measure that window, and RFI-IRFOS did not instrument the app at runtime. Declaring the four google_analytics_default_allow_* keys as false in the manifest closes the window by construction.

Severities in the June notices predate RFI-IRFOS's adoption of CVSS v4.0 on 31 August 2026. This report scores every finding under v4.0. The score above rates the issue as found in June, the status line rates where it stands today.

Fix: Add google_analytics_default_allow_analytics_storage, _ad_storage, _ad_user_data and _ad_personalization_signals with value false to the manifest. No further action needed on the CMP integration.

VC-C1: ViCare: Firebase API key in the APK. UNCHANGED, restriction not verifiable

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N, 6.9

The Firebase key AlzaSyCfv8TY2O7dPsWPdU3X4R2LqYj6KtxtrW0 (project vicare-neu) is unchanged in v3.41.3. Firebase Android keys are identifiers by Google's design. The real exposure depends on API restrictions in Google Cloud and on Firebase Security Rules, which a static review cannot see.

Fix: Confirm that the key is restricted to the Android app signature and to the Firebase APIs ViCare actually calls. No rotation is needed if the restrictions are in place.

VC-H1: ViCare: background location and boot-time geofencing. ACCEPTED

LOW, CVSS v4.0 AV:L/AC:L/AT:P/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 1.8

ACCESS_BACKGROUND_LOCATION and the geofencing boot receiver are unchanged in v3.41.3. Viessmann explained on 2 July 2026 that geofencing is an opt-in, event-based feature of a paid service and that no continuous location track is stored. RFI-IRFOS accepted that explanation. The re-scored value reflects opt-in activation.

VC-H2: ViCare: cleartext permitted in the base network config. ACCEPTED

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

The network security config still permits cleartext in its base configuration and pins viessmann-climatesolutions.com to TLS. Viessmann explained that local diagnostic traffic to the heating unit (DoIP on the local network) requires it. RFI-IRFOS accepted the explanation. All cloud traffic observed in the binary uses TLS.

VC-H3: ViCare: privacy policy does not name every Firebase subsystem. PARTIALLY ADDRESSED**LOW, transparency finding under GDPR Art. 13, not CVSS-scored**

v3.41.3 registers ten Firebase subsystems. The live ViCare privacy policy, read on 26 October 2026, now names Firebase Analytics, Crashlytics and Cloud Messaging, adds a consent requirement for Firebase and Crashlytics, and carries a cookie table. Performance Monitoring, Remote Config and A/B Testing are still not named. Viessmann announced a full revision of the policies for all three apps on 3 September 2026.

VG-C1: ViGuide: Firebase API key in the APK. VERIFIED FIXED (rotated)**MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N, 6.9**

June 2026 (v2.24.7): AlzaSyBltdYgJ7l5uhioeLiTyFF8UhHtL-pWXg4, project vizard-ace22. v2.24.13 ships a different key, AlzaSyDwj9nhwK08PwQ5vUbXWg-79bdpCU-Y4UA. The old key no longer appears anywhere in the APK. Whether the old key was also revoked in Google Cloud cannot be seen from the outside.

VG-C2: ViGuide: Firebase and ML Kit initialised before consent. VERIFIED FIXED**MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 5.1**

v2.24.13 sets firebase_analytics_collection_enabled=false in the manifest and ships the Usercentrics CMP (1,916 SDK strings). Analytics collection now waits for an explicit decision. MLKitNitProvider is still declared. ML Kit runs on-device for the scanner and is not an analytics channel. Viessmann reported this finding to HBDI on 28 July 2026.

VG-H1: ViGuide: app-wide cleartext traffic. VERIFIED FIXED

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

June 2026: android:usesCleartextTraffic="true" on the whole application. v2.24.13 removes the attribute, and the network security config permits no cleartext. Fixed.

VG-H2: ViGuide: KPIT diagnostics host still referenced. OPEN, dormant

LOW, dormant reference with no reachable data flow observed, not CVSS-scored

The string `https://limas.diagnostics.kpit.com` is still present in the dex of v2.24.13. On 9 July 2026 Viessmann stated that this code path is never executed, that the reference would be removed in the next release, and that a signed data processing agreement with KPIT (Munich) is in place. On 3 September 2026 Viessmann listed H2 among the findings addressed in v2.24.9. The KPIT diagnostics library (`com.kpit.*`) is a core component of ViGuide, so a remaining reference is plausible. RFI-IRFOS found no call site that sends data to the host. The removal Viessmann announced has not happened yet.

Fix: Remove the `limas.diagnostics.kpit.com` reference, as announced on 9 July 2026.

VG-H3: ViGuide: data of installation owners processed by a B2B app. ADDRESSED BY STATEMENT

LOW, transparency finding under GDPR Art. 14, not CVSS-scored

ViGuide is used by heating technicians and processes data about the owners of the installations they service. Those owners never see the app. Viessmann stated on 3 September 2026 that app-specific privacy information reaches technicians during Viessmann partner onboarding and at account creation, and that the store listings mark ViGuide and ViParts as business apps. The Art. 14 information of the installation owners themselves runs through the installer relationship. RFI-IRFOS has no evidence against that statement.

VG-M1: ViGuide: password field in a generated toString(). OPEN**LOW, CVSS v4.0 AV:L/AC:L/AT:P/PR:H/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 1.8**

The dex of v2.24.13 still contains the string template EverestGatewayVerificationRequest(password=, which is the signature of a Kotlin data class toString() that prints the password field. If the object is ever logged, the gateway password lands in the log. On 3 September 2026 Viessmann listed M1 among the findings addressed in v2.24.9. String analysis alone cannot tell whether the value is masked at runtime. The template that would print it is still in the binary.

Fix: Override toString() for EverestGatewayVerificationRequest, or mark the field so it is excluded from the generated toString().

VG-M2: ViGuide: internal hosts in the production binary. PARTIALLY FIXED**LOW, information exposure, not CVSS-scored**

The roughly thirty internal Jira URLs found in June are gone in v2.24.13. limas-stage and limas-test2.viessmann.net are still referenced. They reveal environment names and no credentials.

VG-L1: ViGuide: advertising ID permission and Bluetooth scope. UNCHANGED, assessed by Viessmann**LOW, hygiene findings, not CVSS-scored**

com.google.android.gms.permission.AD_ID is still declared. Bluetooth permissions are unchanged and serve the pairing with Viessmann gateways. Viessmann assessed both on 3 September 2026 and placed them in its regular optimisation backlog. allowBackup is true in v2.24.13 (see Residual Risk).

VP-C1: ViParts: Firebase keys in the APK. FIXED for the native key, web key unchanged

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N, 6.9

June 2026 (v1.9.0): native key AlzaSyCO6fpeDUdx9OEoqp2tLe7LgPcBogd8RZo and web key AlzaSyCRKCQ_QCM8ago1dSnmL4RxUed1nIDKi5Q, project vi-its-viparts-prod. v1.11.4 ships a new native key, AlzaSyC2G2WdMMc9Qd6DghdI3DE4rIKUFHezXws. The web key in the bundled JavaScript is unchanged. A Firebase web key is public by design in every web app, so the decisive control is again the API restriction and the Security Rules.

VP-H1: ViParts: Firebase bootstrap before consent. VERIFIED FIXED for Analytics

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 5.1

v1.11.4 keeps analytics collection disabled until consent (analytics_collection_enabled=false). The Firebase Installations registrar is still declared, as it was in June, so the app can still create a Firebase installation ID at start. That ID is a pseudonymous instance identifier, not an analytics event. Viessmann reported this finding to HBDI on 28 July 2026 and shipped the fix in v1.10.2 on 3 August 2026.

VP-M1: ViParts: API gateway key in client JavaScript. VERIFIED FIXED

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N, 6.9

June 2026: backend.apiKey wXVz1og53DQ4dhASEwQClak7Bb5ypen58c in main.2d1ae8e789f01ad9.js, sent to gateway.viessmann-climatesolutions.com/viparts-api. The backend block of v1.11.4 carries only URLs, and the key string appears nowhere in the bundle. Fixed.

VP-M2: ViParts: staging and integration URLs in production. UNCHANGED**LOW, information exposure, not CVSS-scored**

api-staging.viessmann.com and api-integration.viessmann.com are still selectable through the L1/L2/L3 environment switch in the production bundle of v1.11.4. They reveal environment names and no credentials.

VP-M3: ViParts: allowBackup enabled. UNCHANGED**LOW, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.4**

android:allowBackup="true" without dataExtractionRules, unchanged in v1.11.4. App data, including session state, can be copied by adb backup or into the user's cloud backup. Physical or ADB access is required, hence the low score.

VP-L1: ViParts: AD_ID permission and custom-scheme OAuth callback. UNCHANGED**LOW, hygiene findings, not CVSS-scored**

AD_ID is still declared. The IAM login still returns through the custom scheme com.viessmann.viparts:// without a verified App Link, and no PKCE markers were found in the bundle. If the IAM enforces PKCE server-side, the custom scheme is not exploitable. Static analysis cannot confirm that.

Impact Analysis

Before the fix, ViCare started Firebase Analytics on every launch, including the first launch after installation and before any consent dialog. Every ViCare user on Android was affected. The data concerned is device and usage telemetry, not heating data. It still counts as access to terminal equipment under § 25 TDDDG and as processing without a legal basis under GDPR Art. 6 until consent is given.

In ViGuide, app-wide cleartext would have allowed an attacker on the same network (a customer's Wi-Fi in a boiler room, for example) to read or alter unencrypted traffic. Combined with the gateway password data class, that scenario touched installation credentials. Both the cleartext permission and the key are fixed. The toString() template remains, but it only matters if the object is logged.

The ViParts gateway key in JavaScript identified the app to Viessmann's own API gateway. Its scope was never tested. It has been removed.

Today the residual impact is small. What remains is hygiene: internal host names, allowBackup on two business apps, and Firebase keys whose restriction status only Viessmann can see.

The Complete Chain

June 2026, ViCare: install, then first launch, then FirebaseInitProvider starts before Application.onCreate, then Analytics sends app_open and device data, then the consent dialog appears. The consent came after the data.

October 2026, ViCare: install, then first launch, then FirebaseInitProvider starts, then the Usercentrics CMP and Consent Mode v2 hold Analytics until a decision, then data flows only after consent. The only unmeasured part is the gap between provider start and the first setConsent call, which a manifest default would close.

ViGuide in June: technician on a customer network, cleartext permitted app-wide, gateway credentials in a data class with a password-printing toString(). In October: cleartext removed, key rotated, Analytics behind consent. The chain is broken at its first link.

Data Protection, Article by Article

Provision	June 2026	October 2026
GDPR Art. 6(1)(a), § 25(1) TDDDG	Analytics before consent in all three apps	Consent obtained through Usercentrics before Analytics in all three apps
GDPR Art. 13	ViCare policy omitted several Firebase subsystems	Analytics, Crashlytics and Cloud Messaging named, three subsystems still missing, full revision announced
GDPR Art. 14	ViGuide processes data of installation owners	Viessmann relies on partner onboarding and the installer relationship
GDPR Art. 25	Collection on by default	Collection off by default (ViGuide, ViParts), CMP-controlled (ViCare)
GDPR Art. 32	App-wide cleartext (ViGuide), gateway key in JS (ViParts)	Both fixed
GDPR Art. 33	n/a	Viessmann notified HBDI on 2 July and 28 July 2026 on its own initiative

Regulatory Framework

Viessmann's main establishment is in Hesse, so HBDI is the lead supervisory authority under GDPR Art. 56. Viessmann notified HBDI itself. RFI-IRFOS copied HBDI, the Austrian Data Protection Authority (DSB) and the EDPS on the notices and on this closure. Access to terminal equipment falls under § 25 TDDDG in Germany and § 165(3) TKG 2021 in Austria.

ViCare controls heating and heat pump systems. Products with digital elements of this kind fall under the EU Cyber Resilience Act (Regulation (EU) 2024/2847). Its reporting obligations for actively exploited vulnerabilities apply from 11 September 2026, the full requirements from 11 December 2027. The way Viessmann handled this disclosure already matches what the CRA will require.

Indicators of Compromise

No indicator of compromise was observed. The table lists identifiers relevant to monitoring.

Identifier	App	Status
AlzaSyCfv8TY2O7dPsWPdU3X4R2LqYj6KtxtrW0 (vicare-neu)	ViCare	Still in use
AlzaSyBltdYGj7I5uhioeLiTyFF8UhHtL-pWXg4 (vizard-ace22)	ViGuide	Removed from APK, revocation not visible
AlzaSyDwj9nhwK08PwQ5vUbXWg-79bdpCU-Y4UA	ViGuide	Current key
AlzaSyCO6fpeDUdx9OEoqp2tLe7LgPcBogd8RZo (vi-its-viparts-prod)	ViParts	Removed from APK, revocation not visible
AlzaSyC2G2WdMMc9Qd6Dghdl3DE4rIKUFHezXws	ViParts	Current native key
AlzaSyCRKCQ_QCM8ago1dSnmL4RxUed1nIDKi5Q	ViParts	Web key, still in use
wXVz1og53DQ4dhASEwQClAK7Bb5ypen58c (gateway)	ViParts	Removed from bundle
limas.diagnostics.kpit.com	ViGuide	Still referenced, dormant
limas-stage / limas-test2.viessmann.net	ViGuide	Still referenced
api-staging / api-integration.viessmann.com	ViParts	Still referenced

Disclosure Timeline

Date	Event
2026-06-30	R1 ViCare (VC-2026-R1-001) to privacy@ and security@viessmann.com, datenschutz@viessmann-climatesolutions.com and the Carrier data protection contacts
2026-07-02	Viessmann's point-by-point statement on ViCare, HBDI notified the same day
2026-07-02	R1 ViGuide (VG-2026-R1-001) and ViParts (VP-2026-R1-001)
2026-07-09	Viessmann interim status on ViGuide and ViParts, KPIT data processing agreement confirmed
2026-07-28	Viessmann notifies HBDI of ViGuide C2 and ViParts H1
2026-07-29	ViCare 3.39.1 ships Consent Mode v2 with processing denied by default
2026-08-03	ViParts 1.10.2 ships the C1 and H1 fixes
2026-08-12	ViGuide 2.24.9 ships
2026-08-15	RFI-IRFOS asks for a status update
2026-09-03	Viessmann reports all critical findings addressed. RFI-IRFOS replies the same day and announces independent verification
2026-09-28 / 09-30	Embargo dates ViCare / ViGuide and ViParts
2026-10-26	Re-verification against ViCare 3.41.3, ViGuide 2.24.13, ViParts 1.11.4. Report published

Residual Risk & Recommendations

Item	App	Recommendation
KPIT host reference	ViGuide	Remove, as announced on 9 July 2026
Password in generated toString()	ViGuide	Override toString() or exclude the field
Manifest consent defaults	ViCare	Declare google_analytics_default_allow_* as false
Privacy policy, three Firebase subsystems	ViCare	Name Performance Monitoring, Remote Config and A/B Testing in the revised policy
Internal and staging hosts	ViGuide, ViParts	Strip non-production environments from release builds
allowBackup=true	ViGuide, ViParts	Set false or add dataExtractionRules
Firebase key restrictions	All three	Confirm Android signature and API restrictions in Google Cloud
OAuth custom scheme	ViParts	Confirm PKCE is enforced server-side, or move to a verified App Link

None of these items blocks closure. RFI-IRFOS closes REF VC-2026-R1-001, VG-2026-R1-001 and VP-2026-R1-001 as resolved. The apps stay in the weekly APK diff, as every audited app does.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethnergasse 25/10, 8020 Graz, Austria Coordinated disclosure per ISO/IEC 29147. Research activity protected under Austria's Forschungsfreiheitsgesetz (Art. 17 StGG). GDPR Art. 5, 6, 13, 14, 25, 32, 33, § 25 TDDDG. REF VC-2026-R1-001 / VG-2026-R1-001 / VP-2026-R1-001.