



Security & Privacy Disclosure, Final Report

Mein HoT (com.austrianapps.ventocom.hofer)

RFI-IRFOS's cleanest Android case of the 2026 series, by binary standards and by correspondence standards: a controller that replied substantively three times, cited specific statutory authority and a confirmed DPIA for its one Art. 9 processing operation, accepted correction on one point, and left exactly two items open, one still unresolved after a direct question, one newly surfaced during RFI-IRFOS's own continued re-verification and never yet answered

**PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 28
SEPTEMBER 2026, THREE SUBSTANTIVE HUMAN REPLIES RECEIVED, MOST
FINDINGS RESOLVED THROUGH DIALOGUE, ONE ITEM STILL OPEN, ONE NEW
ITEM UNANSWERED**

Target	Ventocom GmbH, 1121 Wien, Austria — Austrian MVNO operator of HoT (Hofer Telekom), network host Magenta/T-Mobile AT, retail channel Hofer/ALDI Sued
Package	com.austrianapps.ventocom.hofer
Platform Audited	Android, static analysis of the production APK (v6.2.0 at R1; independently re-verified by RFI-IRFOS against the then-current v6.3.0 on 2026-09-11)
Initial Disclosure (R1)	2026-06-30, to info@hot.at, BCC Austrian Datenschutzbehörde and EDPS
Disclosure / Embargo Date	2026-09-28
Report Published	2026-10-17
Overall Severity	HIGH
Findings	7 originally disclosed (1 Critical, 3 High, 3 Medium): 2 substantively addressed through correspondence (biometric legal basis and retention; Firebase/RTDB exposure), 1 addressed on the specific technical point raised (Sentry pre-consent init mechanism), 1 remains open (Sentry EU-region migration), 3 Medium findings undisputed; 1 new, unscored item surfaced by RFI-IRFOS's own v6.3.0 re-verification and still awaiting a reply
Correspondence	9 messages sent by RFI-IRFOS over 73 days (2026-06-30 to 2026-09-11), 3 substantive human replies received (2026-08-06, 2026-08-19, 2026-09-11, all from a named HoT Service Team representative at datenschutz@hot.at), plus routine automated receipt confirmations from info@hot.at's ticketing system. RFI-IRFOS's own last message (2026-09-11) raised a new, unscored follow-up point that has not been answered in the 36 days since
Authorities Notified	Austrian Datenschutzbehörde (dsb@dsb.gv.at) · European Data Protection Supervisor (EDPS, edps@edps.europa.eu)

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 and the First Substantive Reply, 6 August 2026	5
4	The Second Substantive Reply, 19 August 2026	6
5	The Third Substantive Reply, 11 September 2026, and RFI-IRFOS's Independent Re-Verification	6
6	Findings	7
6.1	C1: Facial-biometric and ID-document identity verification (Veridas dasFace) for mandatory SIM registration	7
6.2	H1: Hardcoded Firebase/Google API key and Firebase Realtime-Database URL	8
6.3	H2: Crash reporting to Sentry's US ingest endpoint; EU-region migration stated as 'being evaluated' with no date, unchanged as of the most recent re-check	8
6.4	H3: Pre-consent SDK auto-initialization (Firebase / Sentry / ML Kit Content-Providers)	9
6.5	M1: Telecom / eSIM identifier handling (EuiccManager, EID, SubscriptionManager)	10
6.6	M2: Payment and financial data for top-ups via Google Pay (production), mpay24, and Raiffeisen	10
6.7	M3: No custom network-security config, no certificate pinning (cleartext denied by platform default, which is a confirmed positive)	10
7	A New, Unsourced Item: Fine Location Access in v6.3.0, Surfaced 2026-09-11, Unanswered	11
8	The Complete Chain: Disclosure, Three Substantive Replies, Independent Re-Verification, One Open Item, One New Question	11
9	Impact Analysis	12
10	Data Protection – Article by Article	12
11	Regulatory & Legal Landscape	13
12	Indicators of Compromise	13
13	Disclosure Timeline	14
14	Residual Risk & Recommendations	14

Executive Summary

Mein HoT (com.austrianapps.ventocom.hofer) is the self-service, billing, and top-up app for HoT (Hofer Telekom), the Austrian prepaid MVNO operated by Ventocom GmbH (Vienna) on ventocom's white-label Capacitor platform and sold through Hofer/ALDI Sued. RFI-IRFOS's static analysis on 30 June 2026 found an app that, by the standards of this audit series, is clean: no advertising SDKs, no AD_ID, no Privacy Sandbox APIs, no Chinese-origin components, a lean dangerous-permission set, allowBackup disabled, cleartext denied by platform default, and a real in-app GDPR consent service gating Firebase Analytics. One Critical and three High findings remained: a facial-biometric and ID-document identity-verification flow (the Veridas 'dasFace' KYC SDK) used for mandatory Austrian SIM registration, a hardcoded Firebase API key together with a Firebase Realtime Database URL, Sentry crash reporting routed to Sentry's US ingest endpoint, and pre-consent SDK auto-initialization across Firebase, Sentry, and ML Kit.

Ventocom's privacy team (datenschutz@hot.at, signing as 'Dana Weber, HoT Service Team') replied substantively three times: on 6 August, 19 August, and 11 September 2026. The first reply cited the specific statutory basis for the biometric KYC flow (Art. 9(2)(g) GDPR in conjunction with Section 166(2) of the Austrian Telecommunications Act 2021 and Section 5 of the Austrian Identification Procedures Ordinance, which mandates exactly the OCR-plus-facial-match procedure RFI-IRFOS had found) and stated the Firebase key is application-restricted with no live Realtime Database in use. The second reply named the exact manifest configuration (io.sentry.auto-init=false) that gates Sentry's native initializer behind explicit consent, and explained the US Sentry ingest region was a historical artifact of when the organization was first set up, before Sentry offered EU data residency. The third reply confirmed a completed Art. 35(3)(b) DPIA covering the Veridas photoident procedure, and gave specific, verifiable retention figures: deletion at Veridas within seconds to a few minutes of the identification result, with an interim HoT-side storage cap of 72 hours.

RFI-IRFOS independently re-verified Ventocom's claims against the production app rather than accepting them at face value. The Firebase-RTDB claim held up exactly as stated: the FirebaseDatabase class is never instantiated anywhere in the current binary, confirming the hardcoded database URL is dead configuration boilerplate rather than a live attack surface, and RFI-IRFOS said so in the same terms it would have used to report the opposite finding. One item did not hold up: Ventocom's stated intent to evaluate a Sentry EU-region migration had, as of the 11 September re-verification against v6.3.0, produced no migration and no committed date, with the Sentry DSN still pointed at the US/global ingest endpoint. That same re-verification pass also surfaced a new, unscored item outside the scope of the original R1: v6.3.0 declares ACCESS_FINE_LOCATION and ACCESS_COARSE_LOCATION through a functionally wired Capacitor geolocation plugin, a permission the original analysis never addressed because it was not present, or not noticed, in the audited v6.2.0 build.

RFI-IRFOS sent its most recent message on 11 September 2026, closing out the Firebase/RTDB point in Ventocom's favour, restating the unresolved Sentry EU-region question, and raising the new fine-location point as two concrete questions. No reply has arrived in the 36 days since. The embargo set on 30 June 2026 for 28 September 2026 has passed. This report publishes the full record exactly as it stands: a largely resolved, well-documented disclosure with one still-open commitment and one new, unanswered question.

ID	Severity	Title
C1	ADDRESSED	Facial-biometric and ID-document identity verification (Veridas dasFace) for mandatory SIM registration
H1	ADDRESSED	Hardcoded Firebase/Google API key and Firebase Realtime-Database URL
H2	HIGH	Crash reporting to Sentry's US ingest endpoint; EU-region migration stated as 'being evaluated' with no date, unchanged as of the most recent re-check
H3	ADDRESSED	Pre-consent SDK auto-initialization (Firebase / Sentry / ML Kit ContentProviders)
M1	MEDIUM	Telecom / eSIM identifier handling (EuiccManager, EID, SubscriptionManager)
M2	MEDIUM	Payment and financial data for top-ups via Google Pay (production), mpay24, and Raiffeisen
M3	MEDIUM	No custom network-security config, no certificate pinning (cleartext denied by platform default, which is a confirmed positive)

Subject & Operator Context

Ventocom GmbH, headquartered at 1121 Wien, is named verbatim as publisher in the app's own web bundle and is the Austrian MVNO operator running HoT (Hofer Telekom) on the Magenta/T-Mobile AT network, retailed through Hofer/ALDI Sued stores. Ventocom is an EU establishment, so no Art. 27 representative is required, and the Austrian Datenschutzbehörde is the natural lead supervisory authority for an Austrian operator serving Austrian users. The app's KYC vendor, Veridas (das-Nano S.L.), is itself EU-based in Navarra, Spain, a further positive for Chapter V exposure relative to several other targets in this audit series.

Engagement Summary and the First Substantive Reply, 6 August 2026

RFI-IRFOS disclosed seven findings on 30 June 2026 to info@hot.at, BCC the Austrian Datenschutzbehörde and the EDPS, stating an embargo of 28 September 2026. Two follow-ups (17 July, 27 July 2026) drew only automated ticket acknowledgments naming a 1-3 business day response window that had already been exceeded.

On 6 August 2026, datenschutz@hot.at (HoT's actual privacy mailbox, distinct from the general info@hot.at support queue) replied substantively for the first time, addressing all three of RFI-IRFOS's original questions directly: it cited Art. 9(2)(g) GDPR together with Section 166(2) of the Austrian Telecommunications Act 2021 (TKG 2021) and Section 5 of the Identification Procedures Ordinance (IVO) as the specific statutory basis mandating the Veridas photoident procedure, including its OCR-capture and facial-match steps; it confirmed the hardcoded Firebase key is application-restricted and that no Firebase Realtime Database is in live use despite the URL's presence in the binary; and it named datenschutz@hot.at itself as the dedicated data-protection contact point RFI-IRFOS had asked for. RFI-IRFOS replied the same day, accepting the Art. 9(2)(g)/TKG/IVO legal basis for C1 and marking H1 (the Firebase key) as resolved on HoT's own representation, while noting two of the three original questions, the DPIA's existence and the Sentry auto-init mechanism, remained unaddressed.

The Second Substantive Reply, 19 August 2026

After a follow-up on 15 August 2026 restating the two open points, datenschutz@hot.at replied again on 19 August 2026. On the biometric retention question, it pointed to the app's own privacy notice section ('Mandatory Customer Registration under the Telecommunications Act'), which states the photoident selfie is deleted after the procedure concludes per the applicable legal requirements, and confirmed the image is transmitted to Veridas for the identification check itself. On Sentry, it named the exact mechanism disabling pre-consent initialization: the manifest meta-data flag `io.sentry.auto-init=false`, which `SentryInitProvider.onCreate()` checks before calling `SentryAndroid.init()`, meaning the native initializer is a no-op until the application layer explicitly starts Sentry after GDPR consent is obtained. It also explained the US Sentry ingest region (`o56707.ingest.sentry.io`) as a historical artifact: no EU data-residency option existed when Ventocom's Sentry organization was first created.

RFI-IRFOS accepted the auto-init mechanism as a verifiable, specific technical answer and marked H3 (pre-consent SDK init) as addressed on that point. Two items remained: a concrete DPIA confirmation under Art. 35(3)(b) specifically covering the Veridas flow (distinct from the general privacy-notice retention language already given), and a committed position, migrate or don't, with a date, on the Sentry EU-region question.

The Third Substantive Reply, 11 September 2026, and RFI-IRFOS's Independent Re-Verification

After a follow-up on 3 September 2026, datenschutz@hot.at replied on 11 September 2026 confirming that an Art. 35 DPIA had in fact been carried out covering the Section 166(2) TKG 2021 photoident procedure, and gave specific retention figures: deletion at Veridas within seconds to a few minutes of the identification result being determined, with an interim storage cap at Ventocom's own systems of 72 hours for handling any follow-up queries. On Sentry, it stated only that 'the possibility of migrating to the EU region is being evaluated,' with no date and no yes/no answer to RFI-IRFOS's direct question. The reply closed by stating Ventocom considered the matter conclusively resolved.

RFI-IRFOS did not take either claim at face value. It independently re-pulled and re-verified the then-current production build (v6.3.0) before replying the same day. The DPIA and retention answers were accepted as specific and verifiable. The Firebase/RTDB claim from 6 August was independently re-checked at the same time: the `FirebaseDatabase` class is confirmed never instantiated anywhere in the dex bytecode, so the hardcoded database URL is dead configuration boilerplate, not a live exposure, and RFI-IRFOS said so in exactly those terms. The Sentry claim did not hold up to the same scrutiny: the DSN in v6.3.0 still points unchanged at the US/global ingest endpoint, meaning 'being evaluated' had produced no actual migration and no committed timeline, consistent with what HoT's own wording already implied. The same re-verification pass surfaced one new item outside the original R1's scope: v6.3.0 declares `ACCESS_FINE_LOCATION` and `ACCESS_COARSE_LOCATION` through a functionally integrated `@capacitor/geolocation` plugin binding, not a dead SDK remnant, a permission RFI-IRFOS's 30 June analysis never flagged because it was not present, or not noticed, in the audited v6.2.0 build. RFI-IRFOS could not determine the purpose from the binary alone, found indications consistent with a plausible store-locator use case, and asked directly whether the permission existed at the time of the original disclosure or was added since, and under what Art. 6/7 basis if new. No reply has arrived in the 36 days since.

Findings

C1: Facial-biometric and ID-document identity verification (Veridas dasFace) for mandatory SIM registration

ADDRESSED THROUGH CORRESPONDENCE — the Art. 9(1) processing itself is confirmed and remains accurately described; the open legal questions (Art. 9(2) basis, Art. 35 DPIA, retention, transfer destination) were each answered with specific, checkable detail across two replies (2026-08-06, 2026-09-11) rather than disputed

```
assets/capacitor.plugins.json -> @ventocom/capacitor-plugin-veridas-sdks
classes*.dex -> com/veridas (1,432 refs), selfie (323), biometric (119), VDDocument
(28)
assets/public -> https://veridas.com/dasface/schemas/craft-v0.0.0.json
Ventocom, 2026-08-06: Art. 9(2)(g) DSGVO i.V.m. Section 166(2) TKG 2021 und Section 5
IVO (mandatory OCR + facial-match)
Ventocom, 2026-09-11: Art. 35 DPIA confirmed existing; deletion at Veridas within
seconds-minutes, HoT-side cap 72 hours
```

Impact: The app bundles the Veridas KYC SDK (com.veridas, 1,432 references) exposing a dasFace facial-biometric schema, selfie/liveness capture (323 'selfie' and 119 'biometric' references), and government-document capture (VDDocument, passport/rectangle detectors, ML Kit OCR), driven by the camera, to scan an ID document and match it against a live facial capture before a prepaid SIM can be registered. This is processing of biometric data for unique identification under Art. 9(1), confirmed directly from the binary and never in dispute. Ventocom's 6 August 2026 reply supplied the specific Art. 9(2)(g) gateway (substantial public interest) tied to Section 166(2) of the Austrian Telecommunications Act 2021 and Section 5 of the Identification Procedures Ordinance (IVO), which mandates exactly this OCR-plus-facial-match sequence for SIM registration. Its 11 September 2026 reply confirmed a completed Art. 35(3)(b) DPIA covering this specific procedure and gave concrete retention figures: deletion at Veridas within seconds to a few minutes of the identification result, interim storage at Ventocom's own systems capped at 72 hours. RFI-IRFOS did not independently audit the DPIA document itself, which Ventocom stated is not disclosed to third parties, consistent with normal DPIA confidentiality practice; the finding is addressed on the strength of the specific statutory citation, the confirmed DPIA's existence, and the verifiable retention figures given, not on an independent review of the DPIA's contents.

H1: Hardcoded Firebase/Google API key and Firebase Realtime-Database URL

ADDRESSED, INDEPENDENTLY RE-VERIFIED BY RFI-IRFOS — Ventocom's 'application-restricted key, no live RTDB use' claim is confirmed accurate against the current production binary, not merely accepted on their word

```
google_api_key / google_crash_reporting_api_key: [REDACTED IN PUBLIC REPORT --  
disclosed privately to Ventocom GmbH / HoT in R1]  
project_id: hot-at   firebase_database_url: https://hot-at.firebaseio.com  
Ventocom, 2026-08-06: key is application-restricted; RTDB not in live use  
RFI-IRFOS, 2026-09-11, independent re-check of v6.3.0 dex bytecode: FirebaseDatabase  
class never instantiated -- confirmed dead config, claim upheld
```

Impact: A Google/Firebase API key, Firebase app-id, OAuth web client-id, and a Firebase Realtime Database URL (hot-at.firebaseio.com) are extractable verbatim from res/values/strings.xml in every distributed copy of the app. Ventocom's 6 August 2026 reply stated the key is application-restricted and that no Realtime Database is actually in use, so no unauthenticated read/write exposure exists regardless of the URL's presence. RFI-IRFOS did not accept this on faith: on 11 September 2026, re-checking the then-current v6.3.0 binary, RFI-IRFOS confirmed that the FirebaseDatabase class is never instantiated anywhere across the dex bytecode, meaning the database URL is dead configuration boilerplate rather than a live attack surface, and reported this in the same direct language it would have used had the opposite been true. The residual, lower-severity point (an unrestricted or under-restricted key still enables quota/billing-exhaustion abuse against other Firebase services even with the RTDB specifically inert) was not separately re-confirmed or disputed and is noted for completeness, not as an open dispute.

H2: Crash reporting to Sentry's US ingest endpoint; EU-region migration stated as 'being evaluated' with no date, unchanged as of the most recent re-check

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, 7.5 — open as of 2026-09-11, no reply on this point since

```
DSN (assets/public): https://[REDACTED]@o56707.ingest.sentry.io/121487 (US/global  
ingest, not *.ingest.de.sentry.io)  
Ventocom, 2026-08-19: 'no EU data residency available when our Sentry org was created  
'; legal basis cited: Art. 45 EU-US DPF adequacy  
Ventocom, 2026-09-11: 'migration to EU region is being evaluated' -- no date, no  
commitment  
RFI-IRFOS, 2026-09-11 re-check of v6.3.0: DSN unchanged, still o56707.ingest.sentry.io
```

Impact: Sentry crash reporting is integrated natively and in the JS layer, with a DSN pointed at o56707.ingest.sentry.io, Sentry's US/global ingest region, not its EU region. Ventocom's 19 August 2026 reply explained this as a historical artifact (no EU data-residency option existed when the Sentry organization was first set up) and, on legal basis, separately asserted reliance on the EU-US Data Privacy Framework adequacy decision under Art. 45 GDPR rather

than Art. 46 standard contractual clauses; RFI-IRFOS did not independently verify Sentry, Inc.'s DPF certification status against the official registry and reports this as Ventocom's cited basis, not an independently confirmed fact. On 11 September 2026, Ventocom stated only that 'the possibility of migrating to the EU region is being evaluated,' with no yes/no commitment and no date, despite RFI-IRFOS's direct question asking for exactly that. RFI-IRFOS's own re-verification the same day against v6.3.0 confirmed the DSN is unchanged and still points at the US/global endpoint. This finding remains open.

H3: Pre-consent SDK auto-initialization (Firebase / Sentry / ML Kit ContentProviders)

ADDRESSED ON THE SENTRY-SPECIFIC POINT RAISED — Ventocom named a specific, checkable manifest flag (`io.sentry.auto-init=false`) gating native Sentry initialization behind consent; the broader Firebase-FID/ML-Kit initialization-before-consent point was not separately revisited

```
<provider android:name="com.google.firebase.provider.FirebaseInitProvider"/>
<provider android:name="com.google.mlkit.common.internal.MlKitInitProvider"/>
<provider android:name="io.sentry.android.core.SentryInitProvider"/>
Ventocom, 2026-08-19: <meta-data android:name="io.sentry.auto-init" android:value="
    false"/> gates SentryAndroid.init() behind explicit consent
```

Impact: Firebase, ML Kit, and Sentry ContentProviders all declare `directBootAware="true"` and initialize during Application creation, before any consent UI runs, per the AndroidManifest.xml evidence cited in R1. RFI-IRFOS's specific question on the Sentry component was answered on 19 August 2026 with the exact mechanism: the manifest meta-data flag `io.sentry.auto-init=false`, checked by `SentryInitProvider.onCreate()` before it would otherwise call `SentryAndroid.init()`, meaning the native Sentry initializer is a deliberate no-op until the application layer starts it explicitly after GDPR consent. RFI-IRFOS accepted this as a specific, falsifiable technical claim consistent with the rest of Ventocom's generally accurate correspondence and did not independently decompile the consent-gating code path to re-verify it line by line; it is reported as Ventocom's representation, accepted in the live correspondence, not as independently re-run dynamic verification. The broader point, that Firebase Installations (FID) generation and ML Kit's own ContentProvider still run at process start regardless of the Sentry-specific fix, was not raised again by either side after 19 August and remains formally unaddressed, though it was not disputed either.

M1: Telecom / eSIM identifier handling (EuiccManager, EID, SubscriptionManager)

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:R/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.6 — not raised or disputed in correspondence

Impact: The app handles eSIM provisioning (EuiccManager, DownloadableSubscription, the persistent eUICC EID) and SIM/subscription state (SubscriptionManager), plus device info via the Capacitor Device plugin. These are personal data tied to the subscriber requiring a documented Art. 6 basis and Art. 5(1)(c) minimisation; the app's privacy-positive choices (no READ_PHONE_STATE/IMEI, no RECORD_AUDIO, SMS Retriever API rather than READ_SMS) were not undermined by anything in correspondence. This finding was not raised in follow-up correspondence and Ventocom did not address it; it is carried forward unchanged from R1.

M2: Payment and financial data for top-ups via Google Pay (production), mpay24, and Raiffeisen

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:R/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.0 — flagged for completeness, not disputed

Impact: Prepaid top-up payments are processed through Google Pay in production, the Austrian PSP mpay24, and Raiffeisen banking rails. This processing is lawful and largely handled by regulated payment service providers; the finding exists to confirm the privacy notice and Art. 28 processor list correctly name each of these PSPs, which was not addressed in correspondence and is carried forward unchanged from R1.

M3: No custom network-security config, no certificate pinning (cleartext denied by platform default, which is a confirmed positive)

MEDIUM, CVSS v4.0 AV:A/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 4.6 — not raised or disputed in correspondence

Impact: The app ships no custom network_security_config.xml, relying entirely on the targetSdk-36 platform default, which denies cleartext traffic globally, a genuine positive and the reason this app carries no cleartext finding at all unlike several peers in this series. The absence of a custom config also means no certificate pinning on connections to app.hot.at, payment endpoints, or Veridas, which would be expected defence-in-depth under Art. 32 for an app carrying biometric, telecom, and payment data. This finding was not raised in follow-up correspondence and is carried forward unchanged from R1.

A New, Unscored Item: Fine Location Access in v6.3.0, Surfaced 2026-09-11, Unanswered

RFI-IRFOS's 30 June 2026 analysis covered v6.2.0 and found no background location access, listed explicitly as a positive. Re-verifying against the then-current v6.3.0 on 11 September 2026, RFI-IRFOS found the app now declares `ACCESS_FINE_LOCATION` and `ACCESS_COARSE_LOCATION`, wired to a functionally integrated `@capacitor/geolocation` plugin binding rather than dead code, alongside unused Google Maps SDK classes with no configured Maps API key and no Capacitor plugin binding of their own. RFI-IRFOS could not determine the actual purpose from the binary alone; a store or branch locator is a plausible, benign explanation, but this is not confirmed. RFI-IRFOS asked Ventocom directly whether this permission was already present in the audited v6.2.0 build or added since, and if added since, under what Art. 6/7 basis. This is reported here as an open, unscored question, not as a scored finding: RFI-IRFOS does not have enough information from static analysis alone to characterise it as a violation, and assigning it a severity or CVSS score without that information would overstate what is actually known. No reply has arrived in the 36 days since 11 September 2026.

The Complete Chain: Disclosure, Three Substantive Replies, Independent Re-Verification, One Open Item, One New Question

Step 1 – Disclosure sent: RFI-IRFOS discloses seven findings on 30 June 2026 to info@hot.at, BCC Austrian Datenschutzbehörde and EDPS, stating an embargo of 28 September 2026.

Step 2 – Silence beyond automation: Follow-ups on 17 and 27 July 2026 each draw only an automated ticket acknowledgment naming a 1-3 business day window already exceeded.

Step 3 – First substantive reply: On 6 August 2026, datenschutz@hot.at answers with a specific statutory basis for C1 (Art. 9(2)(g) GDPR, TKG 2021 Section 166(2), IVO Section 5) and states the Firebase key is application-restricted with no live RTDB use. RFI-IRFOS marks H1 resolved on HoT's own representation the same day.

Step 4 – Second substantive reply: After a 15 August follow-up, datenschutz@hot.at replies on 19 August 2026 naming the exact manifest flag (`io.sentry.auto-init=false`) gating Sentry's native initializer behind consent, and explains the US ingest region as a historical artifact of when the Sentry organization was created.

Step 5 – Third substantive reply: After a 3 September follow-up, datenschutz@hot.at replies on 11 September 2026 confirming a completed Art. 35 DPIA for the Veridas flow with concrete retention figures, but states only that an EU-region Sentry migration 'is being evaluated,' with no date.

Step 6 – Independent re-verification, not blind acceptance: The same day, RFI-IRFOS re-pulls the then-current v6.3.0 build and checks every claim rather than taking HoT's word for it. The Firebase/RTDB claim holds up exactly as stated. The Sentry claim does not: the DSN is unchanged, still pointed at the US endpoint, confirming 'being evaluated' had produced no actual migration.

Step 7 – A new question surfaces from RFI-IRFOS's own diligence, not from HoT's disclosure: the same re-check finds `ACCESS_FINE_LOCATION/ACCESS_COARSE_LOCATION` newly present and functionally wired in v6.3.0, outside the scope of the original R1. RFI-IRFOS asks directly whether it is new and under what basis.

Step 8 – Silence on what remains open: RFI-IRFOS's 11 September 2026 message, the last in the thread, restates the open Sentry commitment and the new location question. No reply arrives in the following 36 days.

Step 9 – Embargo passes, report publishes: The 28 September 2026 embargo passes. This report publishes 19 days later, documenting three genuine resolutions, one still-open commitment, and one new question exactly as the record stands, neither more resolved nor more adversarial than it actually is.

Impact Analysis

This is, by a wide margin, the most constructively resolved case in RFI-IRFOS's 2026 audit series. Ventocom's privacy team engaged substantively within five weeks of initial silence, cited specific, correct statutory authority for its one genuinely special-category processing operation, confirmed a Data Protection Impact Assessment exists where the law requires one, gave concrete and checkable retention figures, and named the exact manifest flag controlling a disputed initialization timing question. RFI-IRFOS, for its part, did not simply accept these claims: it independently re-pulled and re-checked the production binary twice, confirmed one claim outright (the dead Firebase RTDB class), found one claim had not yet translated into action (the still-unmigrated Sentry US endpoint), and surfaced a new question of its own in the process. The net result is a disclosure that worked close to as intended: findings were investigated, most were resolved with evidence rather than assertion, and the one real outstanding item (Sentry EU-region migration) is narrow, specific, and actionable.

Data Protection – Article by Article

Art. 9(1), 9(2)(g), 35(3)(b), 6, 5(1)(c), 13 GDPR – C1's biometric KYC flow, addressed with a specific statutory basis (TKG 2021 Section 166(2), IVO Section 5), a confirmed DPIA, and concrete retention figures.

Art. 32 GDPR – H1's hardcoded Firebase key and RTDB URL, addressed and independently confirmed inert.

Art. 44, 45, 46, 6(1), 7(1); ePrivacy 5(3) – H2's Sentry US-ingest transfer, remains open on the EU-region migration commitment.

Art. 6(1), 7(1); ePrivacy 5(3) – H3's pre-consent auto-init, addressed on the Sentry-specific mechanism, broader Firebase/ML-Kit point not revisited.

Art. 5(1)(c), 6 GDPR – M1's eSIM/telecom identifier handling, unchanged from R1.

Art. 6(1)(b), 13(1)(e), 28 GDPR – M2's payment-processor disclosure, unchanged from R1.

Art. 32, 25 GDPR – M3's absent certificate pinning, unchanged from R1.

Regulatory & Legal Landscape

Ventocom GmbH is an Austrian establishment, so no Art. 27 EU representative is required and the Austrian Datenschutzbehörde is the natural lead supervisory authority for this Austrian operator serving Austrian subscribers. The EDPS was copied from the original disclosure in BCC per standing RFI-IRFOS practice for cross-border visibility.

Fine exposure under GDPR: Art. 83(5) would apply to the Art. 9 biometric processing in C1 if its legal basis were found inadequate, up to EUR 20,000,000 or 4% of total worldwide annual turnover; however, C1 is treated in this report as addressed, given the specific statutory citation, confirmed DPIA, and concrete retention figures Ventocom provided. Art. 83(4) applies to the Art. 32/44-46 issues that remain open in H2 (Sentry US transfer), up to EUR 10,000,000 or 2% of total worldwide annual turnover, pending Ventocom's committed migration date or a reasoned decision not to migrate.

Indicators of Compromise

The following findings were extracted from static analysis of the production APK (apktool -no-src, strings/grep over dex, the Angular web bundle, and native libraries), independently re-verified twice against subsequent production builds (v6.3.0, 2026-09-11) during the course of correspondence. No Ventocom/HoT servers, accounts, or infrastructure were probed; no dynamic instrumentation was performed. The hardcoded key referenced in H1 is withheld from this public report; the full value was disclosed privately in the original R1 letter.

```
C1 -- Veridas biometric KYC (Art. 9) -- ADDRESSED (statutory basis + DPIA + retention confirmed)
H1 -- Hardcoded Firebase key + RTDB URL -- ADDRESSED (independently re-verified dead config)
H2 -- Sentry US ingest, EU-region migration -- OPEN (no date, no commitment, unchanged as of last check)
H3 -- Pre-consent SDK auto-init -- ADDRESSED on Sentry mechanism (io.sentry.auto-init=false)
M1 -- eSIM/telecom identifiers -- unchanged from R1, not disputed
M2 -- Payment/top-up data (Google Pay, mpay24, Raiffeisen) -- unchanged from R1, not disputed
M3 -- No certificate pinning -- unchanged from R1, not disputed
NEW, unscored -- Fine location access in v6.3.0 -- surfaced 2026-09-11, unanswered 36 days
```

Disclosure Timeline

2026-06-30 Initial disclosure (seven findings) sent to info@hot.at, BCC Austrian Datenschutzbehoerde and EDPS. Embargo stated as 2026-09-28.

2026-07-17, 2026-07-27 Follow-ups sent; both draw only automated ticket acknowledgments.

2026-08-06 First substantive reply from datenschutz@hot.at: Art. 9(2)(g)/TKG/IVO legal basis for C1; Firebase key application-restricted, no live RTDB use. RFI-IRFOS marks H1 resolved on HoT's representation same day.

2026-08-15 Follow-up restating the two remaining open points (DPIA confirmation, Sentry mechanism).

2026-08-19 Second substantive reply: io.sentry.auto-init=false mechanism named; US Sentry region explained as historical, EU-US DPF cited as transfer basis. RFI-IRFOS marks H3's Sentry-specific point addressed.

2026-09-03 Follow-up restating DPIA confirmation and Sentry EU-region migration as the two remaining points, with an Art. 33/72-hour silent-fix monitoring notice standard across this campaign.

2026-09-11 Third substantive reply: Art. 35 DPIA confirmed existing; specific retention figures given; Sentry EU-region migration stated as 'being evaluated,' no date. RFI-IRFOS independently re-verifies against v6.3.0 same day: confirms the Firebase/RTDB claim, finds the Sentry DSN unchanged, and surfaces the new fine-location question. RFI-IRFOS's reply is the last message in the thread.

2026-09-28 Embargo date reached and passed with no further reply.

2026-10-17 This report published, 19 days after the embargo and 36 days after RFI-IRFOS's last message, documenting the resolved items, the one open commitment, and the one new unanswered question exactly as the correspondence record stands.

Residual Risk & Recommendations

C1 – No action required; the statutory basis, DPIA, and retention figures given are specific and adequate on their face. RFI-IRFOS recommends Ventocom continue naming Veridas explicitly as a named processor in its own privacy notice, which it already does.

H1 – No action required for the Realtime Database specifically; general good practice remains to remove the unused firebase_database_url boilerplate from strings.xml to eliminate any future confusion about whether it is live.

H2 – Give either a committed migration date to Sentry's EU region, or a reasoned written statement that migration will not occur and why the US/DPF basis is considered adequate going forward. 'Being evaluated' with no date is not itself a resolution.

H3 – Confirm, if convenient, whether Firebase Installations (FID) generation and the ML Kit ContentProvider are similarly consent-gated, or explain why they are treated differently from Sentry.

New item – Answer whether ACCESS_FINE_LOCATION/ACCESS_COARSE_LOCATION in v6.3.0 existed at the time of the original audit or was added since, its actual purpose, and, if added since, its Art. 6/7 basis.

RFI-IRFOS records this case as substantially resolved through good-faith, evidence-based correspondence, and remains open to a reply on the two remaining points at any time; this report will be updated to reflect one if it arrives.

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 analysis of the published application (apktool -no-src, strings/grep over classes*.dex, the Angular web bundle in assets/public/*.js, and native libraries in lib/arm64-v8a/), independently re-verified twice against subsequent production builds during the course of correspondence (v6.3.0, 2026-09-11). No Vento-com/HoT servers, accounts, or infrastructure were probed; no dynamic instrumentation (Frida) was performed. The hardcoded credential referenced in finding H1 is withheld from this public report; the full value was disclosed privately in the original R1 letter and remains available to the controller or to a supervisory authority on request. Technical evidence is archived under chain of custody. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF HOT-2026-R1-001.