



Security & Privacy Disclosure, Final Report

ivie, the official Vienna city guide (at.vienna.ivie)

Background location described as exact and always, Firebase initialization before the consent banner despite a real consent platform, plaintext City Card data next to an unused encrypted store, and development infrastructure shipped in the production build, answered after 59 days by a cease-and-desist letter that this report documents together with its rejection and the unchanged embargo

PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 4 OCTOBER 2026, TECHNICAL QUESTIONS UNANSWERED

Target	Wiener Tourismusverband (Vienna Tourist Board), Invalidenstraße 6, 1030 Vienna, Austria, public-law body, UID ATU38158907
Package	at.vienna.ivie
Platform Audited	Android · v3.11.1 (versionCode 5912), static analysis of the production APK as analyzed on 2026-07-06
Initial Disclosure (R1)	2026-07-06 (REF at.vienna.ivie)
Disclosure / Embargo Date	2026-10-04
Report Published	2026-10-17
Overall Severity	HIGH
Findings	6 (2 High, 3 Medium, 1 Low)
Correspondence	5 messages sent by RFI-IRFOS, no bounce, 1 cease-and-desist letter from the law firm GEISTWERT on 2026-09-03 (rejected the same day), 1 out-of-office automatic reply, no reply from the operator to the technical questions
Authorities in copy	Austrian Datenschutzbehörde (DSB) - European Data Protection Supervisor (EDPS)

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	5
4	Findings	5
4.1	H1: Background location described to users as exact and always, for a geofence based tips and treasure hunt feature	6
4.2	H2: Firebase initializes through a ContentProvider before the consent banner can render, despite a real consent platform	7
4.3	M1: Vienna City Card data stored in a plaintext local Room database next to an unused encrypted storage layer	8
4.4	M2: Development, staging and demo infrastructure identifiers shipped in the production build	9
4.5	M3: Privacy policy describes Facebook as login only while the binary bundles App Events and install referrer components	10
4.6	L1: Compose preview activity exported in the production release	10
5	Impact Analysis	11
6	The Complete Chain: From Install to Informed Consent	11
7	Data Protection — Article by Article	11
8	Regulatory & Legal Landscape	12
9	Indicators of Compromise	12
10	Disclosure Timeline & Outcome	12
11	What ivie Got Right	13
12	Residual Risk & Recommendations	13

Executive Summary

ivie (at.vienna.ivie, v3.11.1) is the official Vienna city guide app of the Wiener Tourismusverband, built by the developer vendor Exozet, and it served as the host city app for the Eurovision Song Contest 2026. A static analysis of the production APK on 2026-07-06 is a comparatively clean audit within this programme: a real OneTrust consent platform is integrated, no Chinese or Russian SDK and no ad mediation or session replay SDK exists, registration data is minimal, and location uses the efficient geofencing design. The analysis still produced six findings, two HIGH, three MEDIUM and one LOW.

The user facing text describes background location collection as exact and always while the mechanism is event driven geofencing (H1). Firebase initializes before the consent banner can render (H2). Vienna City Card data sits in a plaintext Room table (M1), non-production infrastructure identifiers ship in the release (M2), and the privacy policy describes Facebook as login only while the binary bundles App Events and install referrer components (M3).

The disclosure went to the data protection mailbox on 6 July 2026 with a 90-day embargo of 4 October 2026. Three follow-ups over 49 days drew no reply. The first reaction from the operator side was a cease-and-desist letter from the law firm GEISTWERT on 3 September 2026, which set a deadline of 9 September for a signed undertaking. RFI-IRFOS rejected the claims in full on the same day, declined to sign, and kept the embargo date. No message from the law firm or the operator followed. This report documents that sequence as it happened. The technical questions remain unanswered.

ID	Severity	Title
H1	HIGH	Background location described to users as exact and always, for a geofence based tips and treasure hunt feature
H2	HIGH	Firebase initializes through a ContentProvider before the consent banner can render, despite a real consent platform
M1	MEDIUM	Vienna City Card data stored in a plaintext local Room database next to an unused encrypted storage layer
M2	MEDIUM	Development, staging and demo infrastructure identifiers shipped in the production build
M3	MEDIUM	Privacy policy describes Facebook as login only while the binary bundles App Events and install referrer components
L1	LOW	Compose preview activity exported in the production release

Subject & Operator Context

The Wiener Tourismusverband is a public-law body under the Wiener Tourismusförderungsgesetz, seated at Invalidenstraße 6 in Vienna, with UID ATU38158907, as stated in its public imprint and privacy policy for ivie, both fetched on 2026-07-06. The application entry class com.exozet.dca.App points to Exozet, a digital agency, as developer and processor. That is common industry practice and is not a finding. The Österreichische Datenschutzbehörde is the competent supervisory authority, with no cross-border one-stop-shop question.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 6 July 2026 to datenschutz@wien.info with wtv@wien.info, the Austrian DSB and the EDPS in copy, and fixed a 90-day embargo of 4 October 2026. The disclosure asked yes or no questions about the background location wording, the timing of the Firebase initialization, the Facebook components and the existence of an age or parental consent mechanism for the prize drawing. The last of these was put as a question and not as an assertion. Follow-ups on 23 July, 9 August and 24 August restated the open points and drew no reply.

On 3 September 2026 the law firm GEISTWERT wrote on behalf of the Wiener Tourismusverband with a cease-and-desist letter and a deadline of 9 September 2026 at 12:00 for a signed undertaking. RFI-IRFOS replied the same day, rejected the claims, declined to sign and left the embargo unchanged. Nothing further arrived. This report reflects the state of version 3.11.1 on the date of analysis. Changes the operator made after that date do not alter the historical state, and any change the operator reports will be noted alongside the findings.

Findings

H1: Background location described to users as exact and always, for a geofence based tips and treasure hunt feature

HIGH, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 7.0 — Background location described to users as exact and always, for a geofence based tips and treasure hunt feature

```
onboarding_pushAlert_settingsRedirection_message:
  'ivie collects your exact background location data (always) and needs the permission
  to send notifications, to enable ivies tipsps ...'
ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_BACKGROUND_LOCATION
notification_channel_name: 'ivies tips & challenge notification'
```

```
com/exozet/dca/services/geofence/GeofenceRepository
com/exozet/dca/services/geofence/GeofenceEventProcessor
com/exozet/dca/services/geofence/IvieGeofenceBroadcastReceiver
com/exozet/dca/services/location/GeofenceService
isUserWithinGeofenceRadius, geofenceRadiusInMeters
no periodic high frequency LocationRequest interval found
```

Impact: The app declares ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION and ACCESS_BACKGROUND_LOCATION. Its own permission text tells the user that ivie collects exact background location data, always, for the ivie tips feature, which shares one notification channel with the ESC challenge treasure hunt. The mechanism in the binary is Google's Geofencing API with GeofenceRepository, GeofenceEventProcessor and IvieGeofenceBroadcastReceiver. That is the event driven design the operating system batches, and it is the proportionate engineering choice for a citywide treasure hunt. The finding is the mismatch between that design and the user facing wording. No string narrows always to a limited set of challenge and interest locations, and none names an approximate cadence. Art. 5(1)(c) and Art. 13 both turn on the user being told accurately what is collected and why, and consent under Art. 6(1)(a) is valid only when informed. Either the copy overstates the collection or a broader channel exists, and both readings lead to the same remedy: an accurate and specific description of mechanism, frequency and precision.

H2: Firebase initializes through a ContentProvider before the consent banner can render, despite a real consent platform

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 7.1 — Firebase initializes through a ContentProvider before the consent banner can render, despite a real consent platform

```
<provider com.google.firebase.provider.FirebaseInitProvider initOrder=100
    directBootAware=true exported=false/>
<receiver com.exozet.dca.services.boot.BootUpReceiver exported=true
    permission=RECEIVE_BOOT_COMPLETED> BOOT_COMPLETED </receiver>
no firebase_*_collection_enabled meta-data, no Consent Mode defaults
```

```
res/raw/ot_ui_params.json (OneTrust configuration)
consent_firebase / consent_facebook / consent_adjust / consent_upstream
```

Impact: FirebaseInitProvider is declared with initOrder 100 and directBootAware true. Android instantiates manifest ContentProviders during Application startup, before any Activity and therefore before any consent banner can render. No firebase_analytics_collection_enabled, firebase_crashlytics_collection_enabled or Consent Mode default meta-data gates that start. A BootUpReceiver is exported and fires on BOOT_COMPLETED, protected by the RECEIVE_BOOT_COMPLETED permission and consistent with re-registering geofences after a reboot. The app does integrate OneTrust with a real configuration resource and per vendor categories (consent_firebase, consent_facebook, consent_adjust, consent_upstream), which is deliberate compliance engineering and a genuine mitigation layer. What the binary lacks is a mechanism that places the ContentProvider level initialization behind the consent decision. A Firebase installation ID and a session start therefore exist before the user can act on the banner. Art. 7(1) requires consent to precede processing, and the finding is HIGH and not CRITICAL because a working consent platform is present.

M1: Vienna City Card data stored in a plaintext local Room database next to an unused encrypted storage layer

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.9 — Vienna City Card data stored in a plaintext local Room database next to an unused encrypted storage layer

```
CREATE TABLE cards (id, vccTickets, cardNumber PRIMARY KEY, transactionDate,
    activationDate,
    expirationDate, priceVatRate, bookingCode, card_type_id, card_type_name, type,
    customer_id, firstName, lastName, serviceSales)
encrypted storage present elsewhere: de/adorsys/android/securestoragelibrary/
    SecurePreferences,
    com/exozet/android/core/storage/SecureStorageDelegate
SQLCipher classes: none
```

Impact: A Room table named cards holds the card number (primary key), vccTickets, bookingCode, validity dates, customer_id, firstName and lastName. No SQLCipher class exists in the three dex files, and no evidence shows the database opened through the app's own SecureStorageDelegate or any encryption layer. The same codebase ships a Keystore-backed encrypted storage library (adorsys SecurePreferences wrapped by SecureStorageDelegate) that is used for other data. The capability to encrypt this table exists in the app and, on the binary evidence, was not applied to it. The card is a discount and transit credential and the schema holds no payment card number or CVV, and the realistic threat model is on-device compromise through a lost device or a rooted device, so the finding stays MEDIUM. allow-Backup is false, which blocks adb backup extraction.

M2: Development, staging and demo infrastructure identifiers shipped in the production build

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.9 — Development, staging and demo infrastructure identifiers shipped in the production build

```
firebase_database_url: [REDACTED IN PUBLIC REPORT -- disclosed privately to
    Wiener Tourismusverband in R1]
google_storage_bucket: [REDACTED IN PUBLIC REPORT -- disclosed privately to
    Wiener Tourismusverband in R1]
login_keycloak_link: [REDACTED IN PUBLIC REPORT -- disclosed privately to
    Wiener Tourismusverband in R1]
buy_vcc_stage: [REDACTED IN PUBLIC REPORT -- disclosed privately to
    Wiener Tourismusverband in R1]
wien_demo_shop_base_url: [REDACTED IN PUBLIC REPORT -- disclosed privately to
    Wiener Tourismusverband in R1]
external_link_vcc_test_redeemcode: [REDACTED IN PUBLIC REPORT -- disclosed privately
    to Wiener Tourismusverband in R1]
external_link_vcc_testshop: [REDACTED IN PUBLIC REPORT -- disclosed privately to
    Wiener Tourismusverband in R1]
```

Impact: strings.xml of the production release carries six non-production identifiers: a Firebase Realtime Database URL and a storage bucket of a project named for iOS development, a development identity provider login host, a third-party demo shop domain and two staging hosts of the City Card shop. Staging and development projects are frequently configured with weaker rules than production, and their presence in a consumer build enlarges the attack surface. The hostnames are published as present in the binary. Whether any of them is reachable with production credentials is for the operator to state, and no request was sent to any of them.

M3: Privacy policy describes Facebook as login only while the binary bundles App Events and install referrer components

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.9 — Privacy policy describes Facebook as login only while the binary bundles App Events and install referrer components

```
com.facebook.sdk.ApplicationId, com.facebook.sdk.ClientToken (meta-data)
at.vienna.ivie.FacebookInitProvider
com/facebook/appevents/*, com/facebook/internal/InstallReferrerUtil
consent_facebook: 'Facebook Consent' (app resource)
policy text (wien.info privacy policy, 2026-07-06): Facebook referenced for account
creation only
```

Impact: The operator's published privacy policy for ivie, fetched on 2026-07-06, mentions Facebook for account creation only. The binary declares a Facebook ApplicationId and ClientToken and a FacebookInitProvider that instantiates at process start, and it contains the Facebook App Events package and an InstallReferrerUtil that queries the Play Install Referrer API for attribution. The app's own resources model a consent_facebook category, which shows the operator's design treats Facebook as needing a consent toggle beyond login. Facebook bundles these classes in the same artifact as the login SDK, so their presence alone does not establish which events are transmitted. The finding is the difference between the policy text and the components the binary is provisioned with, and Art. 12 and Art. 13 expect the notice to describe the processing accurately.

L1: Compose preview activity exported in the production release

LOW, CVSS v4.0 AV:L/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.1 — Compose preview activity exported in the production release

```
androidx.compose.ui.tooling.PreviewActivity exported=true
com.google.android.gms.tagmanager.TagManagerPreviewActivity exported=true
```

Impact: Jetpack Compose's design time PreviewActivity ships in the production APK, exported with no permission gate. Google Tag Manager's TagManagerPreviewActivity is also exported, which is its standard component for preview workflows. No data exposure path is shown by either component. This is a build hygiene note for the release configuration of the developer vendor.

Impact Analysis

H1 and H2 concern what the app tells users and when it starts to process. Visitors read that exact background location is collected always, and Firebase has a running installation before they see the consent banner. For a city guide used by tourists and residents during a major international event, the accuracy of the permission text matters because it is the basis of informed consent. M1 concerns a named cardholder's City Card record in a plaintext table on a device that can be lost. M2 and M3 concern build hygiene and the match between the privacy policy and the binary.

One unscored observation concerns the prize drawing of the ESC challenge. The binary shows no age or parental consent text for the drawing, which reuses the general account. This was put to the operator as a question, and it remains one.

The Complete Chain: From Install to Informed Consent

Step 1, Install: Download ivie (at.vienna.ivie) from Google Play.

Step 2, Process start: FirebaseInitProvider and FacebookInitProvider initialize during Application creation, ahead of the OneTrust banner.

Step 3, Consent: OneTrust renders per vendor categories, and the ContentProvider level start is not placed behind them.

Step 4, Location: The permission text promises exact background location, always. The mechanism is geofencing.

Step 5, City Card: A purchased or redeemed City Card is stored with the holder's name in a plaintext Room table.

Step 6, Disclosure: Three follow-ups over 49 days drew no reply, and the first reaction was a cease-and-desist letter.

Data Protection — Article by Article

Art. 5(1)(a) GDPR, fairness and transparency: H2 and M3.

Art. 5(1)(c) GDPR, data minimisation: H1 for the wording of the location collection.

Art. 6(1)(a) and Art. 7(1) GDPR, consent: H1 for informed consent, H2 for consent preceding processing.

Art. 12 and Art. 13 GDPR, information to the data subject: H1 and M3.

Art. 25 GDPR, privacy by design: M1 and M2.

Art. 32(1)(a) and (b) GDPR, security of processing: M1 for encryption at rest, M2 for non-production identifiers, L1 for build hygiene.

ePrivacy Art. 5(3): H2 and M3 for access to terminal equipment.

Regulatory & Legal Landscape

The Österreichische Datenschutzbehörde is the competent supervisory authority for the Wiener Tourismusverband. RFI-IRFOS copied the DSB and the EDPS on the disclosure and on follow-ups. The research is a static analysis of a publicly distributed application, protected as scientific activity under Art. 17 StGG and within the research provisions of Art. 89 GDPR. The reply of 3 September 2026 relied on these provisions and on § 7 UWG for the burden of proof for statements of fact. Each finding is a literal extraction from the distributed binary and can be reproduced with freely available tools.

Indicators of Compromise

The following identifiers were extracted from the production APK (v3.11.1, versionCode 5912, analyzed 2026-07-06) by static analysis only. No server, account or infrastructure of the Wiener Tourismusverband or its vendors was probed.

```
base.apk SHA-256: 663ee6cad33f21b5f2d257410788aaf9d35f78faf8418794957b71e1804f9165
split arm64 SHA-256: 4ae6ec4b38cc495b6c8ae2272f421ef50e1abe05bffa00b2c9e19da9f386793
split xxhdpi SHA-256: 2915202cd1c08226589474b3bb08b83a465c98ee94b90d7a2b50a14fb4fb51dc
```

```
H1  onboarding_pushAlert_settingsRedirection_message, ACCESS_BACKGROUND_LOCATION,
    GeofenceRepository
H2  FirebaseInitProvider (initOrder 100, directBootAware), BootUpReceiver exported
M1  Room table cards (AppDatabase_Impl), no SQLCipher
M2  six non-production identifiers in strings.xml (redacted)
M3  FacebookInitProvider, com/facebook/appevents, InstallReferrerUtil,
    consent_facebook
L1  androidx.compose.ui.tooling.PreviewActivity exported
```

Disclosure Timeline & Outcome

2026-07-06 Initial disclosure (R1, REF at.vienna.ivie) sent to datenschutz@wien.info, with wtv@wien.info, the Austrian DSB and the EDPS in copy. Embargo fixed at 2026-10-04, ninety days after delivery. No bounce.

2026-07-23 First follow-up to datenschutz@wien.info, 17 days after disclosure. No reply.

2026-08-09 Second follow-up, 34 days after disclosure. No reply.

2026-08-24 Third follow-up, 49 days after disclosure. No reply.

2026-09-03 Law firm GEISTWERT Rechtsanwälte, acting for the Wiener Tourismusverband, writes to RFI-IRFOS at 14:00 UTC with a cease-and-desist letter as a PDF attachment, titled as an unfair disparagement of WienTourismus through publication of a root level code analysis, and sets a deadline of 9 September 2026 at 12:00 for a signed cease-and-desist and undertaking declaration. This is the first reaction from the operator side in 59 days, and it addresses none of the technical questions.

2026-09-03 RFI-IRFOS replies at 14:13 UTC to the three lawyers, with the Wiener Tourismusverband data protection mailbox, the Austrian DSB and the EDPS in copy. The reply rejects the claims in full, declines to sign the declaration, points out that the eight weeks of

unanswered questions preceded the letter, states that the public track record page carries a summary of the findings sent on 6 July and that the full report publishes at the embargo date, and leaves the disclosure date of 4 October 2026 unchanged. An out-of-office automatic reply from one of the lawyers arrives 24 seconds later.

2026-09-09 The deadline set by the law firm for the signed declaration passes. No further message from the law firm or from the Wiener Tourismusverband arrives afterwards.

2026-10-04 Embargo date reached. Correspondence record: five messages sent by RFI-IRFOS, no bounce, one cease-and-desist letter from the law firm, one out-of-office automatic reply, no reply from the Wiener Tourismusverband to any of the technical questions.

2026-10-17 This report published, 13 days after the embargo and 103 days after the original disclosure.

What ivie Got Right

A working OneTrust consent platform with a real configuration and per vendor categories is integrated. Location uses Android's event driven Geofencing API and not a polling loop. Registration needs only email, password and name. Camera use is proportionate and tied to a profile photo and the AR challenge. No Chinese or Russian SDK, no ad mediation SDK and no session replay SDK is present. `allowBackup` is false. A Keystore-backed encrypted storage layer exists in the codebase, and screenshot protection is implemented for at least one screen.

These choices do not offset the findings. A consent platform does not move the Content-Provider start behind its banner, and an efficient geofence design does not make the permission text accurate.

Residual Risk & Recommendations

H1 — Replace the wording exact and always with an accurate description of the geofence mechanism, its radius, its precision and its approximate frequency, and document the proportionality assessment.

H2 — Disable Firebase auto initialization in the manifest and start it only after the user's consent decision in OneTrust.

M1 — Open the Room database through the existing encrypted storage layer or SQLCipher.

M2 — Remove development, staging and demo identifiers from the release build and verify that the non-production projects do not accept production credentials.

M3 — Align the privacy policy with the Facebook components in the binary, or remove App Events and the install referrer if unused.

L1 — Exclude Compose tooling from the release build.

Process — State the age and parental consent mechanism, if any, for the prize drawing, and answer the technical questions of the disclosure.

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 at.vienna.ivie

as published on Google Play, analyzed 2026-07-06, using publicly available tools (apktool, unzip, string extraction), and from the operator's public imprint and privacy policy fetched on the same date. No server, account or production infrastructure of the Wiener Tourismusverband or its vendors was probed or accessed. Technical evidence is archived under chain of custody and will be provided to the Österreichische Datenschutzbehörde on request. Research conducted under GDPR Art. 89 (scientific research exemption), ISO/IEC 29147 (coordinated disclosure standard), and the Austrian Federal Constitutional Law Art. 17 (freedom of research). REF IVIE-2026-R1.