



Security & Privacy Disclosure, Final Report

Vinted (fr.vinted) v26.34.1

Four hardcoded Google API keys including a shipped debug credential, four ad/analytics SDKs that auto-initialize before any consent screen can render despite a fully built OneTrust/IAB-TCF CMP, two PRC-origin ad-mediation SDKs bundled without confirmed recipient disclosure, an in-house identity/financial-document capture pipeline with no accredited KYC vendor, an age check scoped only to Wallet payouts, and no demonstrated GPS-stripping path for item photos, unresolved through 112 days and a 20-day-overdue embargo, with zero substantive replies across nine messages

**PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 27
SEPTEMBER 2026, SIX FINDINGS REMAIN UNADDRESSED**

Target	VINTED UAB, Vilnius, Lithuania (second-hand fashion and general-goods marketplace, 100M+ installs)
Package	fr.vinted
Version Audited	v26.34.1 (versionCode 263401), Google Play / APKPure mirror
Platform	Android, static analysis
Initial Disclosure (R1)	2026-06-27 (REF VINTED-2026-R1)
Disclosure / Embargo Date	2026-09-27
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	6 (2 Critical, 3 High, 1 Medium)
Correspondence	9 messages sent by RFI-IRFOS over 112 days (27 June through 11 September 2026) to privacy@vinted.com (hard bounce), dpo@vinted.com (confirmed permanently dead, SMTP 5.1.3), security@vinted.com, press@vinted.com, vinted@vinted.com, and vinted+147240844@vinted.com; nine templated customer-support acknowledgments received, two of them personalize d-but-generic triage replies signed by named support agents ('Anzhelika', 'Alison') asking for more information or confirming a case was 'being checked,' zero substantive reply from a DPO, legal, or security contact addressing any finding
Authorities CC'd / BCC'd	Österreichische Datenschutzbehörde (DSB), Austria; Valstybinė duomenų apsaugos inspekcija (VDAI), Vilnius — lead supervisory authority for VINTED UAB; CERT.at — VDAI (ada@ada.lt) sent a one-line acknowledgment of receipt on 2026-08-31, not a substantive reply

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

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

Contents

1	Executive Summary	4
2	Subject & Operator Context	5
3	Engagement Summary	6
4	Findings	6
4.1	C1: Four hardcoded Google API keys, including a debug-labeled credential shipped in the production build, plus the app's Firebase Realtime Database URL	7
4.2	C2: Four ad/analytics SDKs initialize via manifest initOrder before any consent screen can render, despite a fully implemented OneTrust/IAB-TCF CMP	8
4.3	H1: Two PRC-origin ad-mediation SDKs bundled (ByteDance Pangle, Mintegral) — transparency and Art. 44 questions	9
4.4	H2: High-sensitivity identity/financial documents (ID, bank statement, address proof) processed through an in-house capture pipeline, not an accredited third-party KYC vendor	10
4.5	H3: The only age-verification check found in the binary is scoped to Wallet activation, not to account creation, messaging, or trading	11
4.6	M1: No Vinted-authored code path found that strips GPS/EXIF metadata from uploaded item photos	12
5	Impact Analysis	13
6	The Complete Chain: Nine Messages Across 112 Days, Zero Substantive Replies	14
7	Disclosure Timeline & Outcome	15
8	Data Protection — Article by Article	16
9	Regulatory Landscape & Fine Exposure	17
10	Indicators of Compromise	17
11	Residual Risk & Recommendations	18

Executive Summary

VINTED UAB (Vilnius, Lithuania) operates Vinted, the second-hand fashion and general-goods marketplace with 100M+ installs on Google Play and a 'Parental Guidance Recommended — Users Interact' content rating. A static analysis of fr.vinted v26.34.1 identified six findings, two CRITICAL and three HIGH and one MEDIUM, spanning hardcoded credentials, a structural pre-consent SDK-initialization pattern, undisclosed PRC-linked ad-mediation SDKs, an identity/financial-document capture pipeline built in-house rather than through an accredited vendor, an age check scoped to a single payment flow, and an unconfirmed photo-metadata control.

Four distinct, functioning-format Google API keys are hardcoded verbatim in every distributed copy of the app, including a key explicitly named as a debug-only credential (google_places_api_key_debug) that was not excluded from the production release build, alongside the app's Firebase Realtime Database URL (C1). Separately, the manifest registers four ad/analytics ContentProviders — Google Mobile Ads, AppLovin, Vungle, and Firebase — each with an explicit android:initWithOrder, meaning all four begin initializing before Application.onCreate() runs and therefore before any consent dialog, including Vinted's own genuinely-implemented OneTrust/IAB-TCF v2 CMP, can be displayed (C2). Two PRC-origin ad-mediation SDKs, ByteDance's Pangle and Mintegral, are compiled into the shipped binary, most plausibly reachable through the AppLovin MAX mediation waterfall; recipient disclosure for either named processor could not be confirmed from Vinted's partially machine-rendered privacy policy (H1). Wallet payout activation requires users to photograph and submit identity documents, a bank statement, and proof of address through an in-house-built capture pipeline (KycCameraFragment, KycImageProcessorImpl); a search of the binary for the accredited identity-verification vendors in common use for this exact purpose — Onfido, Jumio, Veriff, iDenfy, Sumsb — returned zero matches (H2). The only age-verification string found anywhere in the resource corpus, 'Must be 18 years or older,' fires exclusively inside the Wallet/KYC flow, not at account registration, browsing, listing, buying, or inside the app's open peer-to-peer messaging system (H3). Finally, no Vinted-authored call path was found anywhere in the two most-reviewed DEX files that strips GPS coordinates from a photo's EXIF data before it is attached to a listing — the only EXIF-handling call sites identified belong to the Glide and CameraX libraries, neither of which touches GPS tags (M1).

RFI-IRFOS disclosed these findings to privacy@vinted.com, security@vinted.com, and press@vinted.com on 27 June 2026, establishing a 90-day coordinated disclosure period with an embargo deadline of 27 September 2026. The original delivery to privacy@vinted.com hard-bounced within seconds (Google Groups: address does not exist); a same-day redelivery to dpo@vinted.com, security@vinted.com, and press@vinted.com followed. Across nine messages sent between 27 June and 11 September 2026 — to the addresses above, to the Lithuanian DPA (ada@ada.lt) and the Austrian DSB (dsb@dsb.gv.at) copied throughout, and to CERT.at blind-copied on the earliest messages — Vinted's own systems returned nine templated acknowledgments, two of them personalized triage replies signed by named support agents asking for more detail or confirming the ticket was 'being checked,' and dpo@vinted.com was separately confirmed to bounce permanently (SMTP 5.1.3) from 24 August 2026 onward. No reply from a DPO, legal counsel, or security contact ever addressed any of the findings substantively. This report publishes 20 days after the embargo deadline, with all six findings unaddressed.

Note on scope: the correspondence above was conducted against the findings identified in RFI-IRFOS's original 27 June 2026 analysis of v26.24.0 — seven advertising/analytics SDKs initializing pre-consent (of which C2's four ContentProviders and H1's two PRC-origin mediation SDKs are the more granular breakdown), a Facebook integration with 3,983 exported

classes, and all four Privacy Sandbox APIs active pre-consent. This report reflects RFI-IRFOS's most current technical analysis, conducted 2026-09-06 against the newer v26.34.1 build, which refines that original scope and adds C1 (hardcoded API keys), H2 (in-house KYC pipeline), H3 (age-gate scope), and M1 (GPS/EXIF handling) as newly documented findings not yet separately communicated to Vinted ahead of this publication.

ID	Severity	Title
C1	CRITICAL	Four hardcoded Google API keys, including a debug-labeled credential shipped in the production build, plus the app's Firebase Realtime Database URL
C2	CRITICAL	Four ad/analytics SDKs initialize via manifest initOrder before any consent screen can render, despite a fully implemented OneTrust/IAB-TCF CMP
H1	HIGH	Two PRC-origin ad-mediation SDKs bundled (ByteDance Pangle, Mintegral) — transparency and Art. 44 questions
H2	HIGH	High-sensitivity identity/financial documents (ID, bank statement, address proof) processed through an in-house capture pipeline, not an accredited third-party KYC vendor
H3	HIGH	The only age-verification check found in the binary is scoped to Wallet activation, not to account creation, messaging, or trading
M1	MEDIUM	No Vinted-authored code path found that strips GPS/EXIF metadata from uploaded item photos

Subject & Operator Context

VINTED UAB, registered office in Vilnius, Lithuania, operates the Vinted marketplace app (fr.vinted) across all Vinted-branded storefronts in the EU and beyond. Vinted's sellers are overwhelmingly private individuals rather than retailers — someone photographing a used item at home, often with family members, children, or domestic details incidentally in frame. This is a materially different privacy posture than a professional seller's studio product shots, and it shapes how the findings below should be weighed: the app's own peer-to-peer messaging system, combined with a Play Store content rating that already flags cross-age user interaction as a risk factor, makes the scope of its one enforced age check (H3) and the absence of a demonstrated photo-metadata control (M1) more consequential than they would be for a retail-only app.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 27 June 2026 to privacy@vinted.com, security@vinted.com, and press@vinted.com, with CERT.at and the Lithuanian DPA (ada@ada.lt) BCC'd. The delivery to privacy@vinted.com hard-bounced within seconds (Google Groups: address does not exist); a same-day redelivery went to dpo@vinted.com, security@vinted.com, and press@vinted.com, same BCC list. A same-day reply to an automated customer-support triage message (signed 'Anzhelika,' asking for more detail) restated that this was a formal GDPR disclosure, not a support ticket, and a further same-day message to vinted@vinted.com — CC'ing dpo@vinted.com and security@vinted.com, BCC'ing the Austrian DSB and the Lithuanian DPA — set out explicitly that the customer-support instruction not to send follow-ups had no legal standing under Art. 77 GDPR and that the 90-day embargo clock, running from 27 June 2026, was unaffected by the volume of automated replies.

Follow-up messages went out on 5 August 2026 (39 days, to dpo@vinted.com and security@vinted.com, CC dsb@dsb.gv.at), 15 August 2026 (49 days, 'dpo@vinted.com now confirmed dead,' to security@vinted.com and vinted@vinted.com, CC dsb@dsb.gv.at and ada@ada.lt), 24 August 2026 (58 days, restating the Art. 33(4) 72-hour notification point), 31 August 2026 (65 days, to vinted+147240844@vinted.com and vinted@vinted.com), and a final message on 11 September 2026 (76 days since disclosure). The Lithuanian DPA (ada@ada.lt) sent a one-line acknowledgment of receipt on 31 August 2026 — confirmation the complaint reached the regulator, not a substantive reply from Vinted. dpo@vinted.com was confirmed to bounce permanently (SMTP 5.1.3, address does not exist) as of 24 August 2026. Across the full 112-day engagement period (27 June through 17 October 2026), Vinted's own systems returned nine templated acknowledgments — two personalized with a named agent's signature but still generic triage language — and no DPO, legal, or security contact ever substantively addressed any of the six findings. This report publishes 20 days after the 27 September 2026 embargo, with no movement on any finding.

Findings

C1: Four hardcoded Google API keys, including a debug-labeled credential shipped in the production build, plus the app's Firebase Realtime Database URL

CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 8.3) — four functioning-format API keys and a Firebase database URL hardcoded verbatim in every distributed copy of a 100M+-install app, one of the four explicitly named as a debug-only credential

```
<string name="default_web_client_id">370947398364-m6308tsifqjtm8a2ur33blvmlubjrurf.
  apps.googleusercontent.com</string>
<string name="firebase_database_url">[REDACTED IN PUBLIC REPORT -- disclosed privately
  to Vinted in R1]</string>
<string name="gcm_defaultSenderId">370947398364</string>
<string name="google_api_key">[REDACTED IN PUBLIC REPORT -- disclosed privately to
  Vinted in R1]</string>
<string name="google_app_id">1:370947398364:android:24ae3262eac318ef</string>
<string name="google_crash_reporting_api_key">[REDACTED IN PUBLIC REPORT -- disclosed
  privately to Vinted in R1]</string>
<string name="google_geo_api_key">[REDACTED IN PUBLIC REPORT -- disclosed privately to
  Vinted in R1]</string>
<string name="google_places_api_key">[REDACTED IN PUBLIC REPORT -- disclosed privately
  to Vinted in R1]</string>
<string name="google_places_api_key_debug">[REDACTED IN PUBLIC REPORT -- disclosed
  privately to Vinted in R1]</string>
<string name="google_storage_bucket">vinted-1041.appspot.com</string>
<string name="project_id">vinted-1041</string>
```

Observed fact vs. inference: the presence of these keys in the binary is an observed fact. Whether they carry effective platform/referrer/package-signature restrictions server-side is the operator's determination under Art. 5(2) accountability, not independently verifiable from the client binary alone. What is independently verifiable is that a debug-labeled key was not excluded from the release build.

Impact: res/values/strings.xml hardcodes four distinct, functioning-format Google API keys (google_api_key, google_crash_reporting_api_key, google_geo_api_key, google_places_api_key) plus a separately-named google_places_api_key_debug key and the app's Firebase Realtime Database URL, extractable from any distributed copy of fr.vinted with apktool in under a minute. The debug-labeled key's presence in the shipped release build is a build-hygiene failure independent of whatever platform or referrer restrictions may or may not be configured server-side on any of the five keys. For a 100M+-install marketplace, quota exhaustion or billing abuse against the underlying Firebase/Maps/Places project can degrade crash reporting, location-based search, and shipping-address features at scale. The app's Google Cloud Storage bucket name (vinted-1041.appspot.com) is likewise now a named, public artifact of this binary; this report does not test its access-control configuration, which would constitute live-backend testing explicitly out of scope for this static pass.

C2: Four ad/analytics SDKs initialize via manifest initOrder before any consent screen can render, despite a fully implemented OneTrust/IAB-TCF CMP

CRITICAL (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, 8.0) — Google Mobile Ads, AppLovin, Vungle, and Firebase all initialize before Application.onCreate(), structurally preceding any point at which a consent dialog could be shown, on every launch, across 100M+ installs

```
<provider android:authorities="fr.vinted.mobileadsinitprovider" android:exported="false"
    android:initOrder="100" android:name="com.google.android.gms.ads.MobileAdsInitProvider"/>

<provider android:authorities="fr.vinted.applovininitprovider" android:exported="false"
    "
    android:initOrder="101" android:name="com.applovin.sdk.AppLovinInitProvider"/>

<provider android:authorities="fr.vinted.vungle-provider" android:exported="false"
    android:initOrder="102" android:name="com.vungle.ads.VungleProvider"/>

<provider android:authorities="fr.vinted.firebaseinitprovider" android:directBootAware="true"
    android:exported="false" android:initOrder="100"
    android:name="com.google.firebase.provider.FirebaseInitProvider"/>

CMP present in the same binary: OTPublishersHeadlessSDK, OneTrustBroadcastReceiver (
    wired into
    MDApplication), IABTCF_TCString / IABTCF_gdprApplies / IABTCF_PurposeConsents /
    IABTCF_VendorConsents / IABTCF_CmpSdkID, IABUSPrivacy_String.

Vinted's own consent-gating logic (MDApplication.onCreate(), smali line 6582) cannot
    execute
until after all four providers above have already completed onCreate().
```

Impact: The manifest declares four ContentProviders — Google Mobile Ads (initOrder="100"), AppLovin (initOrder="101"), Vungle/Liftoff (initOrder="102"), and Firebase (initOrder="100", additionally directBootAware="true") — each of which Android instantiates and calls onCreate() on before Application.onCreate() runs, which in turn runs before any Activity, including a consent dialog, can be displayed. This is documented Android platform behavior, not an inference about Vinted's own code. Vinted ships a genuinely complete consent-management stack alongside this — OneTrust's OTPublishersHeadlessSDK, a wired OneTrustBroadcastReceiver, and full IAB TCF v2 key support — but that CMP cannot gate SDKs whose initialization already completed one Android lifecycle stage earlier, on every single app launch, across a 100M+-install base. This is the same structural pattern this program has confirmed in other audited apps (cf. ViCare/Viessmann C2, 2026-06-30) and is independent of the specific consent text in Vinted's privacy policy.

H1: Two PRC-origin ad-mediation SDKs bundled (ByteDance Pangle, Mintegral) — transparency and Art. 44 questions

HIGH (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, 5.3)
 — two PRC-origin ad-mediation SDKs compiled into the shipped binary, most plausibly reached through the AppLovin MAX mediation waterfall confirmed in C2, creating a transfer-capability risk independent of confirmed live data flow

```
com.bytedance.sdk.openadsdk.activity.TTAdActivity
com.bytedance.sdk.openadsdk.activity.TTRewardVideoActivity
com.bytedance.sdk.component.embedapplog.PangleEncryptManager
...(9 further TTAdActivity-family classes)
```

```
<provider android:authorities="fr.vinted.mbcomponentlifecycleprovider" android:exported="false"
    android:name="com.mbridge.msdk.config.component.status.MBComponentLifecycleProvider"/>
<activity android:exported="false" android:name="com.mbridge.msdk.config.activity.MBRewardVideoActivity"/>
```

Open question, flagged rather than asserted: whether either SDK receives a live ad request

(and therefore a live data flow) during a real user session is not independently confirmed

from this static pass -- mediation networks are typically invoked conditionally by the mediating SDK's runtime waterfall logic. That determination requires live network capture,

explicitly out of scope for this R1 static pass. Whether Pangle or Mintegral are named as

recipients in Vinted's privacy policy could also not be independently confirmed, since the

fetches policy page returned a largely client-rendered locale/string payload rather than

parseable server-rendered prose.

Impact: Two ad-mediation SDKs with PRC corporate origin are compiled into the shipped fr.vinted binary: ByteDance's Pangle (com.bytedance.sdk.openadsdk, the TikTok-parent-company ad network, confirmed via eleven TTAdActivity-family classes and a dedicated PangleEncryptManager) and Mintegral (com.mbridge, formerly Mobvista, confirmed via a registered MBComponentLifecycleProvider and MBRewardVideo activity). Both are most plausibly reached as mediated networks inside the AppLovin MAX waterfall whose own ContentProvider is confirmed present at initOrder="101" (C2) rather than initialized directly by Vinted's own code. Bundling these SDKs is itself an operator decision that creates a capability for advertising-identifier and device-signal data to reach PRC-linked ad-tech infrastructure, triggering Art. 13(1)(e) recipient-disclosure obligations and, where a live data flow occurs, Art. 44-49 third-country transfer requirements.

H2: High-sensitivity identity/financial documents (ID, bank statement, address proof) processed through an in-house capture pipeline, not an accredited third-party KYC vendor

HIGH (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 5.8)
— Wallet payout activation requires government ID, bank statement, and address-proof documents captured through an in-house pipeline; zero dex-string matches for any of the five accredited identity-verification vendors commonly used for this exact purpose

```
com.vinted.feature.kyc.KycCameraFragment
com.vinted.feature.kyc.KycCameraScreenKt
com.vinted.feature.kyc.KycImageProcessorImpl
com.vinted.feature.kyc.KycPhotoTipsFragment
com.vinted.feature.kyc.KycBankStatementEducationFragment
com.vinted.feature.kyc.KycAddressProofEducationFragment
com.vinted.feature.kyc.KycStatusFragment

res/values/strings.xml: id_proof_component_birthday_header_hint,
                        kyc_form_birthday_placeholder,
                        wallet_activation_personal_id_user_too_young_validation
```

Accredited identity-verification vendor search (Onfido / Jumio / Veriff / iDenfy / Sumsb): 0 matches

What this does and does not establish: whether the underlying document verification or fraud-scoring happens server-side via a contracted accredited vendor -- i.e., only the capture

UI is in-house, with images forwarded to a certified backend processor -- is not determinable

from the client binary alone; that requires the operator's own processing-record disclosure.

Impact: Wallet payout activation requires users to photograph and submit a government-issued identity document, a bank statement, and an address proof, using an in-house-built camera/upload flow confirmed in the binary's own `com.vinted.feature.kyc` namespace: `KycCameraFragment`, `KycImageProcessorImpl`, `KycPhotoTipsFragment`, `KycBankStatementEducationFragment`, `KycAddressProofEducationFragment`, `KycStatusFragment`. This program's dex-string search for the accredited identity-verification vendors in common use for this exact fintech/marketplace use case – Onfido, Jumio, Veriff, iDenfy, Sumsb – returned zero matches anywhere in the binary. That the capture UI is in-house-built is a binary fact, drawn directly from Vinted's own class, screen, and image-processor naming. ID documents, bank statements, and proof-of-address are among the most sensitive categories of personal data a consumer app can process, carrying identity-theft and financial-fraud exposure if mishandled, and a DPIA under Art. 35 is very likely mandatory for this processing given its scale and sensitivity.

H3: The only age-verification check found in the binary is scoped to Wallet activation, not to account creation, messaging, or trading

HIGH (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, 5.1) — a 100M+-install marketplace with open peer-to-peer messaging and a Play Store 'Users Interact' content rating enforces an 18+ age check only at the moment a user tries to withdraw money, not at registration, browsing, listing, buying, or messaging

```
<string name="wallet_activation_personal_id_user_too_young_validation">Must be 18
  years or older</string>
```

Scope confirmed present: Wallet/KYC activation flow only

Scope confirmed absent: account registration, browsing, listing, buying, peer-to-peer messaging

Play Store content rating (live listing, fetched 2026-09-06): "Parental Guidance Recommended -- Users Interact"

It remains possible, though not found in this pass, that server-side age inference or a web-based onboarding step outside the APK's own resources performs additional gating -- flagged as an open question rather than asserted absent with certainty.

Impact: The string 'Must be 18 years or older' (wallet_activation_personal_id_user_too_young_validation) is the only age-gate string found anywhere in the resource corpus, and it fires exclusively inside the Wallet/KYC activation flow – i.e., only once a user tries to cash out money. No equivalent string, screen, or validation reference exists for general account registration (whose own strings contain only username/password/zip-code fields, no birthdate field), for browsing, for listing an item, for buying, or for the app's open peer-to-peer messaging system. Vinted's own Play Store listing displays 'Parental Guidance Recommended – Users Interact' as its content rating, meaning Google's own labeling already flags that the app enables direct interaction between users of potentially different ages, unmoderated by Vinted beyond in-app reporting tools. A marketplace combining open unmoderated messaging between strangers, real-money transactions, and a content rating that flags cross-age interaction as a live risk factor, with no enforced age check until a user tries to withdraw money, leaves the messaging and browsing/buying surface unguarded for the exact population the Play Store rating calls out.

M1: No Vinted-authored code path found that strips GPS/EXIF metadata from uploaded item photos

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, 4.2) — the only EXIF-handling call sites found in the two most-reviewed DEX files belong to third-party libraries that never touch GPS tags, with no Vinted-authored GPS-stripping path identified

```
; Glide's own image-header parser -- reads ORIENTATION only, no GPS handling
invoke-direct {p2, p1}, Landroidx/exifinterface/media/ExifInterface;-><init>(Ljava/io/
    InputStream;)V
invoke-virtual {p2, v0, p1}, Landroidx/exifinterface/media/ExifInterface;->
    getAttributeInt(ILjava/lang/String;)I
```

What this does and does not prove, stated explicitly:

- Does not prove GPS data survives into uploaded photos -- that requires a live upload/download round-trip test against the real backend (R2/dynamic scope).
- Does not rule out GPS stripping in a native library -- the arch-specific config.arm64_v8a.apk split was deliberately excluded from this static pass.
- Does not rule out server-side stripping after upload -- invisible to any client-side static analysis by definition.
- Does establish: within the client-side code this program was able to review, there is no demonstrated, Vinted-authored control removing GPS metadata before a photo leaves the device.

Impact: This program searched the two DEX files with the highest density of Vinted's own (com.vinted) classes for any call site into androidx.exifinterface.media.ExifInterface or androidx.camera.core.impl.utils.Exif (CameraX's bundled EXIF utility). The only call site found outside those libraries' own internal implementation was Glide's standard ExifInterfaceImageHeaderParser, which reads only the ORIENTATION tag for correctly rotating a displayed thumbnail – it does not touch GPS tags and does not call removeAttribute. Every GPSLatitude/GPSLongitude/removeAttribute string match found in either disassembled dex resolved to the library classes' own internal constant or method definitions, not to a Vinted-authored caller. Given that Vinted's sellers are overwhelmingly private individuals photographing items inside their own homes, the absence of an affirmatively demonstrated GPS-stripping control is itself the finding: if GPS metadata survives into an uploaded listing photo, it is by default attached to that private seller's home address, and any bystanders in frame become third-party data belonging to someone who never opened the app.

Impact Analysis

The two CRITICAL findings share a structural pattern common to many high-install consumer apps: a genuine, well-built compliance surface (OneTrust/IAB TCF v2 CMP for C2; a real distinction between debug and release credentials implied by the very naming of `google_places_api_key_debug` for C1) sitting alongside an implementation gap that defeats it. C2's four ad/analytics SDKs initialize before Vinted's own CMP can run on every single launch, regardless of what consent-gating logic that CMP contains. C1's debug-labeled key was not excluded from the release build the CMP's own non-debug counterpart ships in. Both are build-and-release-process failures, not failures of intent. H1 compounds C2 by naming two specific PRC-origin recipients whose disclosure status could not be confirmed. H2 and H3 both concern Vinted's Wallet/KYC surface – the single highest-sensitivity data flow in the app – which handles government ID and financial documents through an in-house pipeline and gates age only at that one flow, leaving the rest of a 100M+-install, open-messaging marketplace unguarded by comparison. M1 is the clearest instantiation of third-party bystander data this program found in this binary, given Vinted's seller base skews toward private individuals photographing items in their own homes. That none of the nine messages sent over 112 days drew a single substantive reply from a DPO, legal, or security contact suggests the same process failure this program has observed elsewhere: formal regulatory disclosures are not reaching decision-makers inside the organization, regardless of how the technical findings are received by the customer-support system that intercepts them first.

The Complete Chain: Nine Messages Across 112 Days, Zero Substantive Replies

27 June 2026, 13:09: RFI-IRFOS sends the original disclosure to privacy@vinted.com, security@vinted.com, press@vinted.com, BCC CERT.at and the Lithuanian DPA. privacy@vinted.com hard-bounces within seconds.

27 June 2026, 13:30: Redelivery to dpo@vinted.com, security@vinted.com, press@vinted.com, same BCC list, noting the [privacy@](mailto:privacy@vinted.com) bounce.

27 June 2026, 14:22: Reply to an automated triage message signed 'Anzhelika' asking for more detail, clarifying this is a formal GDPR disclosure, not a support ticket.

27 June 2026, 17:35: R2 clarification to vinted@vinted.com, CC dpo@vinted.com and security@vinted.com, BCC the Austrian DSB and the Lithuanian DPA, stating that the customer-support instruction not to send follow-ups has no legal standing under Art. 77 GDPR and that the embargo clock, running from 27 June, is unaffected by automated-reply volume.

5 August 2026 (39 days): Follow-up to dpo@vinted.com and security@vinted.com, CC dsb@dsb.gv.at, restating the open findings.

15 August 2026 (49 days): Follow-up to security@vinted.com and vinted@vinted.com, CC dsb@dsb.gv.at and ada@ada.lt, noting dpo@vinted.com now confirmed dead.

24 August 2026 (58 days): Follow-up restating the Art. 33(4) 72-hour supervisory-notification point; the copy to dpo@vinted.com bounces permanently (SMTP 5.1.3) the same day.

31 August 2026 (65 days): Follow-up to vinted+147240844@vinted.com and vinted@vinted.com, CC security@vinted.com, dsb@dsb.gv.at, ada@ada.lt. The Lithuanian DPA (ada@ada.lt) sends a one-line acknowledgment of receipt the same day – confirmation the complaint reached the regulator, not a reply from Vinted.

11 September 2026 (76 days): Final follow-up, same recipients, noting eleven days of silence since the previous message and nine automated acknowledgments logged to date.

27 September 2026: Embargo date reached. Correspondence record: nine outreach messages from RFI-IRFOS, nine templated acknowledgments (two personalized but generic) from Vinted, zero substantive engagement with any of the six findings.

17 October 2026: This report publishes, 20 days after embargo, 112 days after the original disclosure. All six findings confirmed unaddressed.

Disclosure Timeline & Outcome

2026-06-27 Initial disclosure sent to privacy@vinted.com (hard bounce), redelivered same day to dpo@vinted.com, security@vinted.com, press@vinted.com. Embargo deadline fixed at 2026-09-27. Four automated acknowledgments received the same day, including one personalized triage reply signed 'Anzhelika' and one signed 'Alison.'

2026-08-05 Follow-up sent, 39 days total, to dpo@vinted.com and security@vinted.com, CC dsb@dsb.gv.at.

2026-08-15 Follow-up sent, 49 days total, to security@vinted.com and vinted@vinted.com, CC dsb@dsb.gv.at and ada@ada.lt. dpo@vinted.com confirmed non-functional.

2026-08-24 Follow-up sent, 58 days total, restating Art. 33(4) GDPR notification point. dpo@vinted.com copy bounces permanently.

2026-08-31 Follow-up sent, 65 days total. Lithuanian DPA (ada@ada.lt) acknowledges receipt of the complaint the same day.

2026-09-06 Follow-up sent, 71 days total, CC press@vinted.com added back; an automated press-inbox acknowledgment follows.

2026-09-11 Final follow-up sent, 76 days total, 16 days before embargo.

2026-09-27 Embargo date reached. Correspondence record shows nine outreach messages from RFI-IRFOS, nine templated acknowledgments from Vinted, zero substantive human reply.

2026-10-17 This report published, 20 days after embargo, 112 days after original disclosure. All six findings unaddressed.

Data Protection — Article by Article

Art. 32(1)(b) GDPR – Security of processing: C1's hardcoded API keys, including a debug-labeled credential shipped in the release build, fall short of the resilience and confidentiality measures Art. 32(1)(b) requires for processing systems.

Art. 25 GDPR – Data protection by design and by default: C1 (a debug credential path not separated from the production path), C2 (a CMP built to gate processing that structurally cannot gate it), H3 (no age-by-design control outside the Wallet flow), and M1 (no demonstrated privacy-by-design control for bystander location data) all implicate Art. 25.

Art. 7(1) GDPR – Conditions for consent: C2's four ad/analytics ContentProviders initialize before any consent dialog can render, meaning whatever consent Vinted's CMP later collects cannot have authorized the processing that already began.

Art. 5(1)(a) GDPR – Lawfulness, fairness and transparency; Art. 5(2) – Accountability: C2's structural pre-consent initialization bears directly on both principles; the burden is on Vinted to demonstrate that the pre-consent window does not itself constitute processing of personal data.

Art. 13(1)(e) GDPR – Recipient disclosure: H1's two PRC-origin ad-mediation SDKs (Pangle, Mintegral) could not be confirmed as disclosed recipients in Vinted's partially machine-rendered privacy policy.

Art. 44-49 GDPR – Chapter V transfers: H1's bundled PRC-origin SDKs raise transfer-safeguard questions conditional on confirmed live data flow.

Art. 35 GDPR – Data Protection Impact Assessment: H2's in-house capture of government ID, bank statements, and address proof at a 100M+-install scale is very likely subject to a mandatory DPIA.

Art. 5(1)(c) GDPR – Data minimization: H2 (is the full bank statement retained, or only the minimum field needed) and M1 (GPS metadata surviving into a listing photo exceeds what is necessary for the marketplace purpose) both implicate data minimization.

Art. 8 GDPR – Conditions applicable to a child's consent: H3's age check, scoped only to Wallet activation, leaves the general registration, messaging, and trading surface unguarded for minors in jurisdictions where the digital age of consent would otherwise require gating.

Regulatory Landscape & Fine Exposure

VINTED UAB is registered in Vilnius, Lithuania, placing it under the jurisdiction and lead supervisory authority of the Valstybinė duomenų apsaugos inspekcija (VDAI, the State Data Protection Inspectorate of the Republic of Lithuania), which acknowledged receipt of this disclosure on 2026-08-31. The Austrian Datenschutzbehörde was copied throughout as the supervisory authority local to RFI-IRFOS. As an EU-registered controller processing EU user data at a 100M+-install scale, Vinted is subject to GDPR's full Article 83 fine structure.

Art. 83(5) GDPR – Maximum fines up to EUR 20,000,000 or 4% of worldwide annual turnover – applies to violations of: Art. 5 (principles), Art. 7 (consent), Art. 25 (data protection by design), Art. 35 (DPIA), and Art. 44-49 (Chapter V safeguards). C2, H1, H2, and H3 each implicate at least one of these articles.

Art. 83(4) GDPR – Maximum fines up to EUR 10,000,000 or 2% of worldwide annual turnover – applies to violations of Art. 32 (security). C1 implicates Art. 32(1)(b) directly.

The scale of Vinted's install base (100M+) is itself a relevant factor under Art. 83(2)(a) (nature, gravity, and duration of the infringement) and Art. 83(2)(k) (number of data subjects affected, degree of damage suffered).

Indicators of Compromise

All findings derive from static analysis of the APK (fr.vinted v26.34.1, SHA-256 of base.apk available on request) as mirrored on APKPure and cross-verified against the live Google Play listing on 2026-09-06. No Vinted servers, accounts, or production infrastructure were probed or accessed.

Residual Risk & Recommendations

C1 – Hardcoded Google API keys: rotate all four affected keys and the debug-only key specifically; verify platform/referrer/package-signature restrictions are configured server-side for each; exclude debug-labeled credentials from release build variants via standard Android build-flavor separation.

C2 – Pre-consent SDK initialization: either remove the android:initOrder declarations and gate ContentProvider initialization behind the OneTrust CMP's own consent-confirmed callback, or adopt Google's own deferred-initialization pattern (delayed app measurement / consent-mode APIs) for each of the four providers so that no ad/analytics SDK executes before a consent decision is recorded.

H1 – PRC-origin ad-mediation SDKs: confirm and publish, in the privacy policy, whether Pangle and Mintegral are live, data-receiving recipients inside the AppLovin MAX waterfall; if so, document the Art. 44-49 transfer safeguard in place, or remove both networks from the mediation configuration.

H2 – In-house KYC pipeline: publish the Art. 35 DPIA for the Wallet identity/financial-document processing flow, or disclose which accredited backend vendor, if any, performs the underlying verification; apply Art. 5(1)(c) minimization review to bank-statement retention specifically.

H3 – Age-gate scope: extend the 18+ age check to account registration, or document the specific legal basis under which minors are permitted to browse, list, buy, and message without an enforced age check.

M1 – GPS/EXIF stripping: add an affirmative, demonstrable GPS-stripping step to the photo-upload pipeline before any listing photo leaves the device, and confirm whether any native-code (.so) path already performs this, since the arch-specific split was out of scope for this static pass.

Process-level improvement: route disclosures via a dedicated, monitored channel separate from the general customer-support queue, and ensure dpo@vinted.com (or its replacement) is kept live and reachable, consistent with the Art. 37(7) obligation to publish and maintain accessible DPO contact details.

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 All findings derive from static analysis of fr.vinted

v26.34.1, the production APK/XAPK as mirrored on APKPure and cross-verified against the live Google Play listing on 2026-09-06, using publicly available tools (apktool, jadx, jq). No Vinted servers, accounts, or production infrastructure were probed or accessed. Technical evidence is archived under chain of custody and will be provided to the VDAI 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 VINTED-2026-R1.