Security & Privacy Disclosure, Final Report

CallApp - Caller ID, Call Blocker, Call Recorder for Android (com.callapp.contacts)

Root level code analysis of the caller-ID/call-recording category; the most substantive correspondence record in this disclosure wave, a postponement request refused, publication text request refused.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO DATE 21 NOVEMBER 2026 REACHED. NO STATEMENT RECEIVED BY THE DEADLINE OF 16 NOVEMBER 2026 AS OF 21 NOVEMBER 2026.

Operator	CallApp Software Ltd., 2 Jabotinsky, Ramat Gan 5250501, Israel
Versions Audited	2.283 / versionCode 2283 (23 Aug 2026, original notice); re-verified against 2.290 (10 Nov 2026, current release, SHA-256 8d4e763581f1a4e3d2f8dd64b04ca15624bda0557d918410158c6b59cb2819f6)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	10: 2 Critical, 5 High, 3 Medium
Status	SUBSTANTIVE CORRESPONDENCE. DPO replied 23 Oct, 1 Nov, 9 Nov. Postponement request refused 2 Nov. Statement opportunity offered, deadline 16 November 2026 passed with no statement received as of 21 November 2026.
SHA-256 (base APK)	`606e2a4f7843b7088472964aee32a9e3b3a42aa6156dcb598365cde1816a9dff`

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 Finding Status at a Glance 6

3 Subject & Operator Analysis 7

4 Architecture & Data Flow 7

5 Engagement Summary 8

6 Findings 8

6.1 C1: Bystander contact data: non-users' information uploaded, processed on legitimate interest, and disclosed to a third party, with no proactive notice mechanism . . . 8

6.2 C2: Binary contradicts the app's own consent screen: Firebase, BidMachine, Vungle initialize via ContentProvider before the consent Activity can render . . 9

6.3 H1: Network security config: cleartext HTTP permitted for every domain, no exceptions, no pinning . . . 10

6.4 H2: Firebase API key and full project configuration hardcoded in distributed binary . . . 11

6.5 H3: Two PRC ad-tech SDKs deeply embedded and auto-initializing pre-consent, on an app holding call-log/contact/SMS permissions . . . 11

6.6 H4: Relationship graph from notifications: dedicated per-platform extractors for WhatsApp, Telegram, Viber, Signal and Vonage, persisted locally . . . 12

6.7 H5: Automatic call recorder with cloud sync records a non-consenting third party's voice, no on-device consent-notice string found . . . 13

6.8 M1: Consent granularity is jurisdiction-inconsistent: Korea gets an itemized overseas-transfer consent step the EU/English flow does not . . . 13

6.9 M2: Marketing claim contradicted by the operator's own Play Store Data Safety declaration . . . 14

6.10 M3: Age mismatch: privacy policy sets a default minimum age of 18, Play Store rates the app Everyone/PEGI 3, no enforced age gate found . . . 14

7 Impact Analysis 15

8 The Complete Chain 15

9 Data Protection: Article by Article 16

10 Regulatory & Legal Landscape 16

11 Indicators of Compromise & Reproducible Evidence 17

12 Disclosure Timeline & Outcome 17

13 What CallApp Got Right 18

14 Residual Risk & Recommendations 19

Executive Summary

CallApp (com.callapp.contacts) is a caller-ID, spam-blocking, call-recording and default-SMS app operated by CallApp Software Ltd., Ramat Gan, Israel, installed on 100M+ Android devices and marketing a crowd-sourced database of "more than 7 billion numbers." On 23 August 2026 RFI-IRFOS disclosed ten findings from a root level code analysis of version 2.283 under REF CALLAPP-2026-R1.

The core finding is structural: CallApp's own code contains a dedicated contact-upload pipeline running as an Android SyncAdapter, and CallApp's own privacy policy confirms, in writing, that phone-book data about people who never installed CallApp ("Contacts") is processed on a legitimate-interest basis, not consent, and is disclosed to a different CallApp user the moment the non-consenting person calls or texts them. A second structural pattern: Firebase, BidMachine and Vungle all initialize via manifest ContentProviders before CallApp's own genuinely detailed first-launch consent screen can render. Layered on top: unrestricted cleartext HTTP network policy, a hardcoded Firebase key, two deeply embedded PRC ad-tech SDKs, a cross-messenger notification-extraction pipeline covering WhatsApp, Telegram, Viber, Signal and Vonage, and an automatic call recorder with cloud sync and no on-device consent-notice string.

CallApp's Data Protection Officer engaged substantively and repeatedly: a first full point-by-point reply arrived 23 October 2026, a second on 1 November 2026, and a third on 9 November 2026. The correspondence is this disclosure wave's most developed exchange. CallApp has defended the core caller-ID data flow on the merits (the "peephole" analogy: a user is entitled to know who is contacting them) rather than disputing the underlying facts, which RFI-IRFOS has not found persuasive for the reasons set out in the Data Flow discussion below, and that disagreement is recorded as a stated position on both sides rather than resolved.

On 1 November 2026 CallApp requested a one-month postponement of publication, citing "the current sensitive security situation in Israel." RFI-IRFOS refused on 2 November 2026: the 21 November 2026 publication date, fixed on 23 August 2026, does not move. On 9 November 2026 CallApp asked to review the publication text in advance and comment on it before release. RFI-IRFOS refused this on 10 November 2026, citing the programme's equal-treatment rule that no company sees its entry before publication, while offering CallApp the opportunity to submit its own written statement by 16 November 2026 for verbatim, unedited reproduction under the label "CallApp's position." The deadline of 16 November 2026 passed, and as of 21 November 2026 that statement has not arrived. A final notice of 15 November 2026 titled 6 days to publication also drew no reply.

Scope: Root level code analysis of the Google Play release bundle 2.283 (base APK SHA-256 above; APKPure mirror, cross-verified live against the Google Play Store listing) and a re-pull of the current release 2.290 on 10 November 2026 (SHA-256 8d4e763581f1a4e3d2f8dd64b04ca15624bda0557d918410158c6b59cb2819f6): manifest, resources, and dex-string/grep inventory over all 8 dex files. Passive review of CallApp's own public privacy policy and live Play Store Data Safety declaration. No CallApp backend, account, or API key was probed or tested.

ID	Severity	Title
C1	CRITICAL	Bystander contact data: non-users' information uploaded, processed on legitimate interest, and disclosed to a third party, with no proactive notice mechanism
C2	CRITICAL	Binary contradicts the app's own consent screen: Firebase, BidMachine, Vungle initialize via ContentProvider before the consent Activity can render
H1	HIGH	Network security config: cleartext HTTP permitted for every domain, no exceptions, no pinning
H2	HIGH	Firebase API key and full project configuration hardcoded in distributed binary
H3	HIGH	Two PRC ad-tech SDKs deeply embedded and auto-initializing pre-consent, on an app holding call-log/contact/SMS permissions
H4	HIGH	Relationship graph from notifications: dedicated per-platform extractors for WhatsApp, Telegram, Viber, Signal and Vonage, persisted locally
H5	HIGH	Automatic call recorder with cloud sync records a non-consenting third party's voice, no on-device consent-notice string found
M1	MEDIUM	Consent granularity is jurisdiction-inconsistent: Korea gets an itemized overseas-transfer consent step the EU/English flow does not
M2	MEDIUM	Marketing claim contradicted by the operator's own Play Store Data Safety declaration
M3	MEDIUM	Age mismatch: privacy policy sets a default minimum age of 18, Play Store rates the app Everyone/PEGI 3, no enforced age gate found

Finding Status at a Glance

ID	Disclosed	This report	Status as of 21 November 2026
C1	CRITICAL	CRITICAL	CallApp disputes the legal characterization (the ”peephole” analogy), not the underlying data flow. Position recorded on both sides; finding stands.
C2	CRITICAL	CRITICAL	CallApp confirmed the structural fact (SDKs initialize before the consent screen) on 23 Oct; no named technical control closing the gap has been given as of 10 Nov, across versions 2.283 and 2.290.
H1	HIGH	HIGH	CallApp committed to a network security config change ”in the upcoming month” (9 Nov reply); unverified in the shipped binary as of 10 Nov (still 2.290, unchanged).
H2	HIGH	HIGH	Not separately contested; stands as disclosed.
H3	HIGH	HIGH	CallApp states both PRC vendors’ terms reference SCC Module 1 (9 Nov reply); whether transfers occur pre-consent was not answered, per RFI-IRFOS’s 10 Nov reply.
H4	HIGH	HIGH	Not separately contested; stands as disclosed.
H5	HIGH	HIGH	Not separately contested; stands as disclosed.
M1	MEDIUM	MEDIUM	Not separately contested; stands as disclosed.
M2	MEDIUM	MEDIUM	Not separately contested; stands as disclosed.
M3	MEDIUM	MEDIUM	Not separately contested; stands as disclosed.

Subject & Operator Analysis

CallApp Software Ltd. is registered at 2 Jabotinsky, Ramat Gan 5250501, Israel. A named Data Protection Officer (dpo@callapp.com) engaged with this notice more substantively than any other target in this disclosure wave, with full point-by-point replies on 23 October, 1 November and 9 November 2026. An EU representative contact, eurep@callapp.com, has been copied on CallApp's own replies since 23 October 2026, closing what RFI-IRFOS's original findings had flagged as an unverified Art. 27 gap. On 1 November 2026 CallApp requested a one-month postponement of the publication date, citing "the current sensitive security situation in Israel" affecting the company's work and resources; RFI-IRFOS declined on 2 November 2026, holding to the 21 November 2026 date fixed on 23 August 2026. On 9 November 2026 CallApp asked to review and comment on the publication text before release; RFI-IRFOS declined this on 10 November 2026 under its standing equal-treatment rule, while inviting CallApp to submit its own written statement by 16 November 2026 for verbatim reproduction.

Architecture & Data Flow

CallApp's own code contains a dedicated contact-upload pipeline (uploadContacts start/uploadContacts end, a full com.callapp.contacts.sync.* package with SyncManager, SyncAdapter and platform-specific syncers) backed by the Android account-sync-adapter permission set (GET_ACCOUNTS, READ_SYNC_SETTINGS, WRITE_SYNC_SETTINGS, READ_SYNC_STATS). CallApp's own privacy policy states that this uploaded "Contacts" data, about people who never installed CallApp, is processed on a legitimate-interest basis and disclosed to a CallApp user the moment the non-consenting person calls or texts them, retained for as long as that person interacts with a CallApp user. Firebase, BidMachine and Vungle are declared as manifest ContentProviders (directBootAware="true", initOrder="100"/"102"), structurally initializing before any Activity, including CallApp's own first-launch consent screen. A NotificationListenerService with dedicated extractor classes for WhatsApp, Telegram, Viber, Signal and Vonage builds a locally persisted communications-relationship graph (ObjectBox entity ExtractedInfo). A re-pull of the current release, version 2.290, on 10 November 2026 found the Firebase/BidMachine/Vungle provider declarations unchanged from 2.283, and additional ad-mediation providers present (InMobi, Meta Audience Network, Fyber FairBid, Bigo Ads, MobileFuse), of which only MobileFuse carries a documented auto-init-disable manifest flag (com.mobilefuse.sdk.disable_auto_init=true); none of the five SDKs named in RFI-IRFOS's question carries an equivalent switch.

Engagement Summary

The original notice went to dpo@callapp.com and support@callapp.com on 23 August 2026. A follow-up on 12 September 2026, twenty days later, had received no reply or acknowledgment of any kind. A 35-days-to-publication notice went out 17 October 2026, fifty-seven days without a reply. CallApp's DPO sent the programme's first substantive reply on 23 October 2026 (now copying eurep@callapp.com), addressing each finding point by point; RFI-IRFOS answered the same day, accepting two factual precisions (a second deletion route by email, and that the five-year retention period in Section 7 of CallApp's privacy policy applies to unlisting rather than deletion) while holding the core finding open. CallApp replied again on 1 November 2026, maintaining its position on the data flow and requesting a one-month postponement of publication citing the security situation in Israel. RFI-IRFOS refused the postponement on 2 November 2026 and set a 9 November 2026 deadline for three named-mechanism questions. CallApp answered on 9 November 2026, committing to a network-security-config change "in the upcoming month" and citing SCC Module 1 for its two PRC ad-tech vendors, while asking to review the publication text in advance. RFI-IRFOS's final reply, sent 10 November 2026, declined the pre-publication review under the programme's equal-treatment rule, offered a 16 November 2026 deadline for CallApp's own verbatim statement, and reported the findings of a fresh pull of the then-current release (2.290), which left the core architecture unchanged.

Findings

C1: Bystander contact data: non-users' information uploaded, processed on legitimate interest, and disclosed to a third party, with no proactive notice mechanism

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:N/SA:N, 7.5 (CVSS-B), rated CRITICAL by blast-radius escalation

RFI-IRFOS blast-radius escalation: raised from HIGH/7.5 to CRITICAL because this is CallApp's own marketed core feature, operating at the scale of a claimed 7 billion numbers, confirmed in writing by the operator's own privacy policy, and because three rounds of correspondence with CallApp's own Data Protection Officer left the underlying legal-basis and notice-mechanism questions unresolved rather than closed.

```
"Information regarding contacts contained in user device phone books ('Contacts')
    [...] will be
collected and processed by CallApp"
"Collected Information regarding users' Contacts will be disclosed to a user if a
    Contact tries
to communicate with the user (by call, SMS, etc.)"
"We will retain and use Contact's information, as long as he/she interacts with a user
     of the
Service, unless he/she requests to be unlisted or deleted."
```

CallApp's 23 October 2026 reply offered a peephole analogy: a CallApp user looking through a digital peephole before deciding whether to answer. RFI-IRFOS's answer the same day: a peephole shows a visitor as they stand at the door: this shows a name a different person

saved in their own phone book and that CallApp uploaded from there, something the caller did not provide and in most cases does not know exists. Calling from a blocked number, CallApp's suggested avoidance route, places the burden of avoiding the processing on the person the processing is about, not on CallApp.

On Art. 14(5)(b) (CallApp's proposed exception from the duty to notify the data subject directly): RFI-IRFOS's 23 October 2026 reply cited the Article 29 Working Party's transparency guidelines (WP260 rev.01, endorsed by the EDPB), which state this exception should not be routinely relied upon by a controller that is not processing for archiving, research or statistical purposes, and that the effort of direct notice must be weighed against the impact on the data subject. CallApp holds a working phone number for every person concerned; a published privacy policy reaches people who already know CallApp exists, not the bystander this finding is about. CallApp's 1 November 2026 reply accepted two precisions (a second deletion route by email within 30 days, and that the five-year retention figure applies to unlisting, not deletion) and the correction that 7 billion counts numbers, not people, while maintaining its position on the data flow itself.

Impact: A bystander, a journalist's source, a domestic-abuse survivor's contact, a patient, anyone ever saved in another person's phone book, has their name and number disclosed to a stranger the moment they call or text that person, on an operator's own legitimate-interest basis, with no notice to them at the point their data enters a database described as covering 7 billion numbers.

Fix: Open, positions recorded on both sides as of CallApp's reply of 9 November 2026.

C2: Binary contradicts the app's own consent screen: Firebase, BidMachine, Vungle initialize via ContentProvider before the consent Activity can render

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), CVSS scores technical exploitability and gives a pure pre-consent timing defect 0.0

Firebase, BidMachine and Vungle are declared as ContentProviders (directBootAware="true", initOrder="100"/"102"), structurally guaranteed by Android's own component lifecycle to initialize before any Activity, including CallApp's own first-launch consent screen. This stands unchanged in version 2.290, re-verified 10 November 2026.

```
<provider android:authorities="com.callapp.contacts.firebaseinitprovider" android:
    directBootAware="true"
          android:exported="false" android:initOrder="100" android:name="com.google.
    firebase.provider.FirebaseInitProvider"/>
<provider android:authorities="com.callapp.contacts.bidmachineinitprovider" android:
    exported="false"
          android:initOrder="100" android:name="io.bidmachine.BidMachineInitProvider
    "/>
<provider android:authorities="com.callapp.contacts.vungle-provider" android:exported
    ="false"
          android:initOrder="102" android:name="com.vungle.ads.VungleProvider"/>
```

CallApp's 23 October 2026 reply confirmed the structural fact and argued initialization is not collection. RFI-IRFOS's answer: Art. 5(3) of the ePrivacy Directive does not turn on whether personal data is collected, it turns on whether information is stored on or read from the device,

and the CJEU held in Planet49 (C-673/17) that this applies whether or not that information is personal data. CallApp's 9 November 2026 reply named only that ad SDKs read a TCF consent string from local storage once one exists, citing an InMobi support page; InMobi is not one of the three named SDKs, and RFI-IRFOS's 10 November 2026 reply noted that in version 2.290 only one ad SDK in the binary (MobileFuse) carries a documented auto-init-disable flag, and it is not among the three.

Impact: Every installation runs Firebase, BidMachine and Vungle initialization before the device owner has seen or made a consent choice, on every cold start including the very first one, with no named technical control closing that gap as of the 9 November 2026 reply.

Fix: Open as of 10 November 2026; CallApp has committed to a network security config change but has not named a corresponding SDK-timing control.

H1: Network security config: cleartext HTTP permitted for every domain, no exceptions, no pinning

---

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), rated HIGH by blast-radius escalation

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.3 to HIGH because the single base-config rule applies to every network destination the app talks to (its own backend, Firebase, AdMob, BidMachine, Vungle, Meta Audience Network, Pangle, Mintegral, PubMatic) on an app holding READ_CALL_LOG, READ_CONTACTS, READ_SMS, WRITE_SMS and call-recording audio permissions.

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <base-config cleartextTrafficPermitted="true" />
</network-security-config>
```

Corroborated by Google Play's own Data Safety section for this listing, retrieved live 23 October 2026: "Data isn't encrypted. Your data isn't transferred over a secure connection." CallApp's 9 November 2026 reply committed to a change in "the upcoming month." Version 2.290, pulled 10 November 2026, still ships the identical single base-config rule.

Impact: Every network destination this app talks to, carrying call-log, contact and SMS-derived data, is permitted to transmit over unencrypted HTTP with zero domain restriction and zero certificate pinning, and the committed fix had not shipped as of the 10 November 2026 re-check.

Fix: Committed by CallApp for an unspecified future release; not yet shipped in version 2.290 as of 10 November 2026.

H2: Firebase API key and full project configuration hardcoded in distributed binary

LOW, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N, 2.1 (CVSS-B), rated HIGH by blast-radius escalation

RFI-IRFOS blast-radius escalation: raised from LOW/2.1 to HIGH because this key sits in the same binary as the contact-upload and call-recording-sync pipelines (C1, H5) of a 100M+-install default-SMS and caller-ID app, where an availability failure removes a user's active spam-call protection.

```
<string name="google_api_key">AIzaSyBDt3u_cvb0rqCdlC5pL-9i0rdPiLyXPds</string>
<string name="google_crash_reporting_api_key">AIzaSyBDt3u_cvb0rqCdlC5pL-9i0rdPiLyXPds
    </string>
<string name="firebase_database_url">https://callapp-com-callapp-apis.firebaseio.com</
    string>
<string name="google_app_id">1:448940416822:android:ab96169860866065</string>
<string name="project_id">callapp.com:callapp-apis</string>
<string name="gcm_defaultSenderId">448940416822</string>
<string name="default_web_client_id">448940416822-h4js1umh9vmtoovpj1cv7jv32l9hpmtb.
    apps.googleusercontent.com</string>
<string name="admob_app_id">ca-app-pub-4050499156041921~8536864490</string>
```

Impact: The key can be used to probe or exhaust project quotas for the callapp.com:callapp-apis project, and to attempt reads against the associated Firebase database and web client configuration, extractable in seconds from any copy of the distributed binary.

Fix: Open; not separately raised in CallApp's replies.

H3: Two PRC ad-tech SDKs deeply embedded and auto-initializing pre-consent, on an app holding call-log/contact/SMS permissions

HIGH, CVSS scoring does not apply cleanly to a data-minimization and transfer-safeguard transparency finding; 0.0 (CVSS-B), assessed qualitatively as HIGH given the permission scope and reference density

ByteDance Pangle and Mintegral are integrated with full mediation-SDK depth (4,101 and 5,652 distinct string references respectively across the dex set, not stub dependencies), each with its own ContentProvider/Activity components reachable at process start, on an app holding READ_CALL_LOG, READ_CONTACTS, READ_SMS and WRITE_SMS.

```
"bytedance" -> 4,101 distinct string references   "pangle" -> 109
"mbridge"   -> 5,555 distinct string references   "mintegral" -> 97
api16-access-sg.pangle.io, api16-access-ttp.tiktokpangle.us, www.pangleglobal.com,
analytics.us.tiktok.com, log.byteoversea.com
```

CallApp's 9 November 2026 reply stated that the terms and conditions of both Pangle and Mintegral reference the Standard Contractual Clauses, Module 1, and reiterated that no personal data is collected before consent. RFI-IRFOS's 10 November 2026 reply noted this names a safeguard class but does not name whether any transfer to these vendors occurs

before the consent screen has rendered, which is the question asked; a vendor's own terms describing its general practice is that vendor's statement, not a control CallApp built into its own app, and the manifest-level auto-init-disable flag found in version 2.290 belongs to a different SDK (MobileFuse) entirely.

Impact: Two PRC-jurisdiction ad-mediation vendors are integrated at full mediation depth and reachable from process start on an app whose core permission set covers call logs, contacts and SMS, without an EU-equivalent itemized transfer-consent step of the kind CallApp has already built for its Korean user base.

Fix: Open as of 9 November 2026; CallApp has named a general SCC class for both vendors but not confirmed pre-consent transfer status.

H4: Relationship graph from notifications: dedicated per-platform extractors for WhatsApp, Telegram, Viber, Signal and Vonage, persisted locally

---

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:N/SA:N, 7.5 (CVSS-B)

A NotificationListenerService with per-platform extractor classes for WhatsApp, Telegram, Viber, Signal and Vonage reads the OS-rendered notification banner for each incoming IM call or message and persists the extracted sender identity to a local ObjectBox entity (ExtractedInfo) tagged with a RecognizedPersonOrigin, independent of CallApp's stated caller-ID purpose.

```
Lcom/callapp/contacts/manager/NotificationExtractors/WhatsAppNotificationDataExtractor
    ;
Lcom/callapp/contacts/manager/NotificationExtractors/TelegramNotificationDataExtractor
    ;
Lcom/callapp/contacts/manager/NotificationExtractors/ViberNotificationDataExtractor;
Lcom/callapp/contacts/manager/NotificationExtractors/SignalNotificationDataExtractor;
Lcom/callapp/contacts/manager/NotificationExtractors/VonageNotificationDataExtractor;
Lcom/callapp/contacts/model/objectbox/ExtractedInfo;
```

This capability powers the "New Caller ID for WhatsApp, Viber and Telegram calls" feature in CallApp's own 21 August 2026 changelog. Because NotificationListenerService reads the notification as the OS already rendered it, this reaches past each messenger's own encryption and metadata-minimization design at the point of display, including Signal, an app whose entire threat model is built around minimizing exactly this kind of externally observable metadata. Not separately raised in CallApp's three replies.

Impact: A communications-relationship graph spanning five independent messaging platforms, who contacts the device owner, by which platform, how often, is built and persisted on-device by a caller-ID app whose stated purpose is identifying phone callers, not messaging-app relationship mapping.

Fix: Open; not separately raised in CallApp's replies.

H5: Automatic call recorder with cloud sync records a non-consenting third party's voice, no on-device consent-notice string found

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:N/SA:N, 7.5 (CVSS-B)

A resource search across every string in res/values/strings.xml for a user-facing "this call is being recorded" announcement, or any instruction to obtain the other party's consent before recording, returns no matches. The CallRecordingSyncer class (in the same sync package as C1) confirms recordings are backed up to the cloud, matching the Play Store listing's own text.

The Play Store description places the entire compliance burden on the user ("users should check and follow local laws before recording any conversation") without the app providing any in-call mechanism to discharge that burden. The person recorded on the other end of the call is, in the large majority of cases, not a CallApp user and never saw any consent screen, the same bystander-data pattern as C1, but for voice audio synced to cloud storage. Not separately raised in CallApp's three replies.

Impact: A non-consenting third party's voice is recorded and synced to cloud storage with no in-app announcement mechanism, in jurisdictions including Austria (Section 120 of the Criminal Code) and Germany (Section 201) that require all-party consent to record a private conversation.

Fix: Open; not separately raised in CallApp's replies.

M1: Consent granularity is jurisdiction-inconsistent: Korea gets an itemized overseas-transfer consent step the EU/English flow does not

MEDIUM, CVSS scoring does not apply to a disclosure-consistency transparency finding; 0.0 (CVSS-B)

res/values/strings.xml contains a standalone Korean-language "Consent to overseas data transfer" dialog string (국외 이전 동의), required by Korea's PIPA, with no equivalent standalone international-transfer consent string in the English resource set, which bundles everything into a single "Agree & continue" action.

Impact: CallApp has built the capability to present a specific, itemized cross-border-transfer consent step and applied it only to the Korean market, despite GDPR Art. 44 to 49 imposing comparable transfer-specific transparency obligations on EU users.

Fix: Open; not separately raised in CallApp's replies.

M2: Marketing claim contradicted by the operator's own Play Store Data Safety declaration

MEDIUM, CVSS scoring does not apply to a self-contradiction transparency finding; 0.0 (CVSS-B)

CallApp's own Play Store description states "We do not sell, share data with any third party application and/or organization," while the same listing's developer-submitted Data Safety section states "This app may share these data types with third parties: Device or other IDs." Both statements are authored and submitted by the same operator, on the same store page, at the same time.

Impact: A prospective user reading the marketing text and the operator's own self-certified Data Safety declaration on the same store page receives two contradictory answers to the same question from the same company.

Fix: Open; not separately raised in CallApp's replies.

M3: Age mismatch: privacy policy sets a default minimum age of 18, Play Store rates the app Everyone/PEGI 3, no enforced age gate found

MEDIUM, CVSS scoring does not apply to an age-assurance consistency finding; 0.0 (CVSS-B)

CallApp's privacy policy states the service "is not designed or intended for children under the age of eighteen (18)" with a reactive, discretionary age-verification clause, while the same app carries a PEGI 3/Everyone Play Store content rating. No age_gate, date_of_birth, dob_, coppa or parental string was found anywhere in res/values/strings.xml.

Impact: An app whose own privacy policy sets an 18-year eligibility threshold is distributed with an all-ages store rating and no client-side mechanism found in the binary that would enforce that threshold at install or first launch.

Fix: Open; not separately raised in CallApp's replies.

Impact Analysis

The population most exposed by C1, H4 and H5 is not CallApp's own 100M+ account holders but the people in those holders' phones, and the people who call or message them, who never installed CallApp at all: a journalist's source, a domestic-abuse survivor's contact, a patient, anyone ever saved in someone else's address book or recorded on the other end of a call. C2's pre-consent SDK initialization affects every one of the 100M+ installs on every cold start, regardless of jurisdiction, and remained structurally unchanged in the 10 November 2026 re-pull of version 2.290. H1's absent network restriction is a materially larger MITM surface on an app holding call-log, contact and SMS read/write permissions than on an ordinary app.

The Complete Chain

Point of contact: a CallApp user grants READ_CONTACTS during setup, pulling in their entire phone book, spouses, children, doctors, employers, exes, sources, informants, anyone they have ever saved a number for. Processing: the sync.* package's SyncAdapter framework uploads that phone book, including the entries of people who never installed CallApp, classified and matched against a claimed 7-billion-number database, while Firebase, BidMachine and Vungle have already begun initializing via ContentProvider before the user's own consent screen renders. Disclosure: per CallApp's own privacy policy, the uploaded bystander's name and number are disclosed to the CallApp user the moment that bystander calls or texts them. Defense offered: CallApp frames this as a peephole, the user's own right to know who is contacting them. Consequence for the bystander: their name and number now sit in CallApp's systems, disclosed to a stranger, with no notice sent to them at the point of upload, and their only route out is a self-service web form or a support email they would have to already know to send, for a product they never installed and a company whose existence they likely do not know.

Data Protection: Article by Article

- Art. 5(1)(a): fairness toward the non-user bystander whose data is uploaded and disclosed without their knowledge (C1).
- Art. 6(1)(f): legitimate interest as the stated legal basis for processing a non-user's contact data, with no documented balancing test produced in three rounds of correspondence (C1).
- Art. 14, Art. 14(5)(b): no proactive notice mechanism to the bystander at the point their data is uploaded; CallApp's reliance on the publication-of-the-privacy-policy exception does not meet the WP260 standard that this exception not be routinely relied upon outside archiving, research or statistical processing (C1).
- Art. 5(3) ePrivacy Directive (via Planet49, C-673/17): storing or reading information on a device before a consent choice is made is in scope regardless of whether that information is personal data, which is why CallApp's "initialization is not collection" position does not answer the question (C2).
- Art. 7(1): processing (including SDK initialization) before consent is obtained (C2).
- Art. 32(1)(a)/(b): absence of any domain restriction or certificate pinning in the network security config, on an app processing call-log, contact and SMS data (H1); resilience of processing systems independent of key-secrecy classification (H2).
- Art. 44 to 46: transfer safeguards for two PRC ad-tech vendors where CallApp has named a general SCC Module 1 reference but not confirmed pre-consent transfer status (H3).
- Art. 5(1)(c): data minimization, questioning why a caller-ID app needs a cross-messenger relationship graph (H4) or two independent PRC ad-mediation stacks (H3).

Regulatory & Legal Landscape

CallApp Software Ltd. is an Israeli entity. RFI-IRFOS's original findings flagged an unverified Art. 27 EU representative gap; CallApp's correspondence has copied eurep@callapp.com since 23 October 2026, which this report records as the EU representative contact rather than restating the earlier gap as unresolved. Absent a confirmed EU main establishment, the Austrian Datenschutzbehörde remains the Austrian-initiated lead contact for this correspondence, with the EDPS in copy per standing practice. All GDPR article citations above are exact; no NISG or AI Act citation applies to this target.

Indicators of Compromise & Reproducible Evidence

Artifact	Value
Package	com.callapp.contacts
Base APK SHA-256 (2.283)	606e2a4f7843b7088472964aee32a9e3b3a42aa6156dcb598365cde1816a9dff
XAPK container SHA-256 (2.283)	c2cb2377019c7c3dfa152440bbc67bb09e9ffb82fdaa6721819ab0c486ec1196
Base APK SHA-256 (2.290, re-pull 10 Nov)	8d4e763581f1a4e3d2f8dd64b04ca15624bda0557d918410158c6b59cb2819f6
Firebase API key	AIzaSyBDt3u_cvb0rqCdIC5pL-9i0rdPiLyXPds
Firebase project	callapp.com:callapp-apis (app ID 1:448940416822:android:ab96169860866065)
EU representative contact (confirmed in correspondence)	eurep@callapp.com

Disclosure Timeline & Outcome

23 August 2026: original notice to dpo@callapp.com and support@callapp.com. 12 September 2026: follow-up, twenty days, no reply or acknowledgment. 17 October 2026: 35-days-to-publication notice, fifty-seven days without a reply. 23 October 2026: CallApp's DPO sends the programme's first substantive, point-by-point reply, now copying eurep@callapp.com; RFI-IRFOS answers the same day, accepting two factual precisions and holding the core finding open, narrowing to three remaining questions. 1 November 2026: CallApp replies again, maintains its position on the data flow, and requests a one-month postponement of publication citing the security situation in Israel. 2 November 2026: RFI-IRFOS refuses the postponement in writing, publication stays 21 November 2026, and sets a 9 November 2026 deadline for the three remaining questions. 9 November 2026: CallApp answers, naming SCC Module 1 for its two PRC vendors and committing to a network-security-config change "in the upcoming month," and separately asks to review and comment on the publication text in advance. 10 November 2026: RFI-IRFOS declines the pre-publication review under its equal-treatment rule, reports findings from a fresh pull of version 2.290 (core architecture unchanged), and offers CallApp a 16 November 2026 deadline to submit its own written statement for verbatim reproduction under the label "CallApp's position." 15 November 2026: final notice titled 6 days to publication from s.kepp@rfi-irfos.com in the same thread, naming 21 November 2026 as the publication date. 16 November 2026: the deadline for CallApp's written statement passes. As of 21 November 2026 no statement and no other message from CallApp has been received, and the report is published.

What CallApp Got Right

- The most substantive, sustained engagement of any target in this disclosure wave: three full point-by-point replies from a named Data Protection Officer, each addressing specific findings rather than a form response.
- A genuinely detailed, itemized first-launch consent screen exists and honestly enumerates the categories of data processed, including call and message metadata, more candid than most targets in this programme, even though its timing relative to SDK initialization (C2) undercuts its effect.
- A working, named, self-service phone-number ”Unlist” mechanism exists at callapp.com/unlist, plus a confirmed second route by email to support@callapp.com, a genuine dedicated opt-out pathway for non-users that most crowd-sourced caller-ID competitors do not offer transparently at all.
- A named Data Protection Officer contact and, per the correspondence record, a working EU representative contact (eurep@callapp.com).
- Google Funding Choices / IAB TCF v2 decoding is integrated for ad-personalization consent signaling.
- No ACCESS_BACKGROUND_LOCATION is requested; location access is foreground-only.
- No CAMERA permission is requested despite the app’s broad communications feature set.
- A specific, itemized overseas-data-transfer consent step was built for the Korean market, demonstrating the underlying capability exists even though it has not been extended to EU users (M1).
- Explicit, documented retention periods are stated in the privacy policy rather than left undefined.

Residual Risk & Recommendations

Two findings carry a concrete, dated commitment from CallApp: a network security config change ”in the upcoming month” (H1, as of the 9 November 2026 reply) and a general SCC reference for its two PRC ad-tech vendors (H3), neither confirmed in the shipped binary as of the 10 November 2026 re-pull of version 2.290. The core findings, C1’s bystander data flow and C2’s pre-consent SDK initialization, are recorded as a disagreement on the merits between CallApp’s peephole framing and RFI-IRFOS’s analysis, not a dispute over the underlying facts, which CallApp has confirmed. RFI-IRFOS continues weekly binary diffing against the archived builds through publication. CallApp’s invitation to submit its own written statement, reproduced verbatim under the label ”CallApp’s position,” expired on 16 November 2026 with no statement received.

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 Root level code analysis of the published Google

Play release bundle plus the operator’s own public legal documents and written correspondence. No CallApp servers, accounts, or API keys were probed or tested. Research conducted under ISO/IEC 29147 and the freedom of scientific research (Art. 17 StGG). Final report, published 21 November 2026. REF CALLAPP-2026-R1.