



Security & Privacy Disclosure, Final Report

Coinbase (com.coinbase.android) v14.24.32

Google Consent Mode defaults hardcoded to granted with no consent mechanism anywhere in the binary, an Android Privacy Sandbox configuration open to every app on the device, a hardcoded Firebase key with a live database URL, and a screen-recording-capable SDK in a financial app, met by one bug-bounty redirect, six automated acknowledgments and a ticket closure that called the correspondence a pressure pattern while leaving all three questions unanswered

PUBLIC DISCLOSURE, 17 OCTOBER 2026. EMBARGO REACHED 30 SEPTEMBER 2026, TWO CRITICAL FINDINGS UNADDRESSED ON THE MERITS

Target	Coinbase Global, Inc. and its EU entities: Coinbase Luxembourg S.A. (CSSF-authorized MiCA crypto-asset service provider since June 2025) and Coinbase Ireland (e-money services); Data Protection Officer dpo@coinbase.com
Package	com.coinbase.android (versionCode 142400320)
Platform	Android, static analysis (base.apk 209.7 MB, 12 classes*.dex files, React Native and Expo based)
Initial Disclosure (R1)	2026-07-02 (REF CB-2026-R1-001)
Disclosure / Embargo Date	2026-09-30
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	4 (2 Critical, 1 High, 1 Medium) plus 1 Low configuration note and 1 negative result
Correspondence	7 messages sent by RFI-IRFOS over 61 days (2 July through 1 September 2026) to security@coinbase.com and dpo@coinbase.com, with the Austrian DSB, the EDPS and the Luxembourg CNPD in copy. Six were written follow-ups; one (2 July, 11:24 UTC) was an automatic Gmail emoji reaction to the Security redirect and contained no text. Coinbase responded with eight messages: six identical automated acknowledgments from the DPO inbox (2 July twice, 9 August, 24 August, 31 August, 1 September), one reply from security@coinbase.com on 2 July redirecting to the HackerOne bug-bounty program, and one Jira service-desk closure of ticket SECURITY-517761 on 1 September, written by a Coinbase staff member, resolving the matter as 'Fixed / No Further Action' on the basis of the 2 July redirect. The ticket characterized the correspondence as consistent with a disclosure-pressure pattern; the same ticket states that independent technical verification of the underlying claims is tracked separately. None of the three questions was answered. Three delivery failures occurred: cnpd@cnpd.lu rejected mail on 2 July and 9 August (address not found), and edps@europa.eu, a mistyped address in the 9 August copy list, rejected mail on 9 August; the correct address edps@edps.europa.eu was used in every other message.
Authorities CC'd	Österreichische Datenschutzbehörde (DSB), Austria; European Data Protection Supervisor (EDPS); Commission Nationale pour la Protection des Données (CNPd), Luxembourg (address rejected mail on both attempts)
SHA-256 (base APK)	b0a7217dd4ca1309fe09c01f8928c0bd80655230badd5bdb2a81c27759c3e6cb

Contents

1	Executive Summary	4
2	Subject & Operator Context	5
3	Engagement Summary	5
4	Findings	6
4.1	C1: Google Consent Mode defaults hardcoded to granted; no consent mechanism in the binary; Firebase auto-initializes before the first screen	6
4.2	C2: Android Privacy Sandbox (AdServices) configured to allow every app on the device to access all three attribution surfaces	7
4.3	H1: Firebase API key and Realtime Database URL hardcoded in plaintext	8
4.4	M1: Datadog Session Replay SDK compiled into a financial application; production activation and field masking not determined (R1 label: H2)	8
4.5	L1: No network_security_config.xml and no certificate pinning; platform default relied upon	9
5	Impact Analysis	9
6	The Complete Chain: Seven Messages Sent, Eight Responses, Zero Answers	10
7	Disclosure Timeline & Outcome	11
8	Chinese-Vendor SDK Thesis: Tested, Not Confirmed	11
9	What Coinbase Got Right	12
10	Data Protection Article by Article	12
11	Regulatory Landscape & Fine Exposure	13
12	Indicators of Compromise	13
13	Residual Risk & Recommendations	13

Executive Summary

Coinbase's Android application (com.coinbase.android v14.24.32) was analyzed on 2 July 2026 with apktool, an independent aapt2 manifest dump and string extraction across all 12 dex files. The analysis identified two CRITICAL findings, one HIGH finding and one MEDIUM finding, plus one LOW configuration note and one documented negative result (the Chinese-vendor SDK thesis was tested and not confirmed).

C1: all seven Google Analytics and Firebase Consent Mode meta-data values are hard-coded to granted in the manifest (analytics storage, ad storage, ad user data, ad personalization signals, ad ID collection, Firebase analytics collection), FirebaseInitProvider auto-initializes at initOrder 100 before the first Activity, and an exhaustive search of all resources and meta-data keys found no consent-management platform of any kind (OneTrust, Didomi, Usercentrics, IAB TCF, Cookiebot and ConsentManager all returned zero matches). The only consent strings in the binary belong to the Onfido identity-verification flow. C2: res/xml/ad_services_config.xml sets allowAllToAccess to true on all three Android Privacy Sandbox surfaces (attribution, custom audiences, topics), while the app requests all four Ad-Services permissions. H1: a Firebase API key and a live Realtime Database URL sit in plaintext in strings.xml.

Coinbase's published posture contains real strengths, recorded below: a CSSF-issued MiCA licence with EU-wide passporting, a published DPO contact and a privacy rights dashboard, process-isolated Onfido KYC components, foreground-only location, allowBackup disabled and cleartext blocked by platform default. The contrast between the licensing and contractual maturity and the shipped consent configuration is the central observation of this case.

RFI-IRFOS put three yes or no questions to Coinbase on 2 July 2026 and repeated them on 9 August, 24 August, 31 August and 1 September. Coinbase's Security team answered once with the standard bug-bounty redirect, the DPO inbox answered six times with the same automated text, and on 1 September a service-desk ticket closed the matter without answering any question. After 107 days and an embargo that passed 17 days ago, C1 and C2 remain unaddressed on the merits. This report is the public record of that state.

ID	Severity	Title
C1	CRITICAL	Google Consent Mode defaults hardcoded to granted; no consent mechanism in the binary; Firebase auto-initializes before the first screen
C2	CRITICAL	Android Privacy Sandbox (AdServices) configured to allow every app on the device to access all three attribution surfaces
H1	HIGH	Firebase API key and Realtime Database URL hard-coded in plaintext
M1	MEDIUM	Datadog Session Replay SDK compiled into a financial application; production activation and field masking not determined (R1 label: H2)
L1	LOW	No network_security_config.xml and no certificate pinning; platform default relied upon

Subject & Operator Context

Coinbase is one of the largest regulated crypto-asset exchanges and publishes com.coinbase.android on Google Play. In the European Union it operates through Coinbase Luxembourg S.A., which holds a CSSF-issued MiCA authorization with passporting across all 27 member states (June 2025), and Coinbase Ireland for e-money services. A data protection officer is publicly reachable at dpo@coinbase.com and a self-service privacy rights dashboard exists. A company with this licensing and contractual maturity sets the benchmark against which a hardcoded granted state for every Consent Mode signal, and the absence of any consent mechanism in the binary, are measured.

Engagement Summary

RFI-IRFOS analyzed com.coinbase.android v14.24.32 on 2 July 2026 using apktool (manifest and resources, memory-safe pass without baksmali), raw string extraction across all 12 classes*.dex files and an independent aapt2 xmltree and badging cross-check of the manifest. base.apk SHA-256: b0a7217dd4ca1309fe09c01f8928c0bd80655230badd5bdb2a81c27759c3e6cb. Coinbase's own legal pages returned HTTP 403 to automated fetch, so statements about its privacy policy rest on search-indexed excerpts and public press material and are marked accordingly. No Coinbase servers, accounts or production infrastructure were probed or accessed.

The initial disclosure went out on 2 July 2026 at 10:01 UTC to security@coinbase.com and dpo@coinbase.com, with the Austrian DSB, the EDPS and the CNPD in copy, fixing a 90-day embargo of 30 September 2026. It listed four findings (C1, C2, H1, H2) and three yes or no questions on awareness of the Consent Mode defaults, the Article 28 agreement with Datadog for the Session Replay module, and whether the findings would be remediated before or after the Austrian data protection authority makes contact. The message also contained an optional commercial advisory offer; public disclosure was stated to proceed independently of any response.

Open R2 items are documented in the Residual Risk section: a cold-start network capture to confirm live transmission before any consent action, a live test of the Firebase key, a cross-app AdServices access test and a scoped decompile of the Datadog Session Replay initialization.

Findings

C1: Google Consent Mode defaults hardcoded to granted; no consent mechanism in the binary; Firebase auto-initializes before the first screen

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, 6.9 - every Consent Mode v2 signal ships as granted and no code path exists to deny it

```
<meta-data android:name="firebase_analytics_collection_enabled" android:value="true"/>
<meta-data android:name="firebase_analytics_collection_deactivated" android:value="
  false"/>
<meta-data android:name="google_analytics_adid_collection_enabled" android:value="true
  "/>
<meta-data android:name="google_analytics_default_allow_analytics_storage" android:
  value="true"/>
<meta-data android:name="google_analytics_default_allow_ad_storage" android:value="
  true"/>
<meta-data android:name="google_analytics_default_allow_ad_user_data" android:value="
  true"/>
<meta-data android:name="google_analytics_default_allow_ad_personalization_signals"
  android:value="true"/>

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

Impact: The manifest sets `google_analytics_default_allow_analytics_storage`, `google_analytics_default_allow_ad_storage`, `google_analytics_default_allow_ad_user_data` and `google_analytics_default_allow_ad_personalization_signals` to true, together with `google_analytics_adid_collection_enabled` and `firebase_analytics_collection_enabled`. These are the literal keys Google's Consent Mode v2 documentation specifies for declaring the default consent state before a user chooses. Setting the ad user data and ad personalization signals defaults to granted is the pattern European supervisory authorities have identified as defeating the purpose of Consent Mode. `FirebaseInitProvider` (`initOrder` 100, `directBootAware`) is instantiated during process creation, before the first Activity and therefore before any consent screen. An exhaustive search of all meta-data keys and string resources found zero matches for OneTrust, Didomi, Usercentrics, IAB TCF, Cookiebot and ConsentManager; the only consent strings belong to Onfido's KYC flow. Observed fact: the shipped configuration declares consent as granted for every category and provides no mechanism to reach a denied state. Not observed: live transmission of events to Google before any user action, which requires a network capture. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to CRITICAL because the configuration is a built-in permanent yes for every user of a regulated financial application, which makes valid consent under Art. 4(11) and Art. 7 structurally impossible from first launch, a consequence the CVSS technical scope does not capture.

C2: Android Privacy Sandbox (AdServices) configured to allow every app on the device to access all three attribution surfaces

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, 5.1 - allowAllToAccess true on attribution, custom audiences and topics, with all four AdServices permissions requested

```
<?xml version="1.0" encoding="utf-8"?>
<ad-services-config>
  <attribution allowAllToAccess="true" />
  <custom-audiences allowAllToAccess="true" />
  <topics allowAllToAccess="true" />
</ad-services-config>
```

Impact: res/xml/ad_services_config.xml sets allowAllToAccess to true for attribution, custom-audiences and topics, the most permissive setting of the Privacy Sandbox access policy. Any other app or SDK on the device, and not only Coinbase's own declared partners, can query Coinbase's attribution reports, custom-audience membership and derived ad-topic data through the platform's own APIs. The manifest also requests ACCESS_AD SERVICES_ATTRIBUTION, ACCESS_ADSERVICES_AD_ID, ACCESS_ADSERVICES_CUSTOM_AUDIENCE and ACCESS_ADSERVICES_TOPICS next to the legacy AD_ID permission, so the configuration is in active use. Observed fact: this exact file ships in the release build. Whether another app has read Coinbase-derived data in practice was not tested. RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.1 to CRITICAL because this is an explicit data-protection-by-default decision (Art. 25) made for every user of a financial application, in the same build that hardcodes consent as granted (C1), which compounds the two findings into a single absence of user control over advertising data.

H1: Firebase API key and Realtime Database URL hardcoded in plaintext

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:L/SC:N/SI:N/SA:N, 7.1 - anonymous quota exhaustion and user enumeration are possible with the key alone; database rules were not tested

```
<string name="google_api_key">[REDACTED IN PUBLIC REPORT -- disclosed privately to
  Coinbase in R1]</string>
<string name="firebase_database_url">[REDACTED IN PUBLIC REPORT -- disclosed privately
  to Coinbase in R1]</string>
<string name="project_id">[REDACTED IN PUBLIC REPORT -- disclosed privately to
  Coinbase in R1]</string>
```

Impact: res/values/strings.xml contains the Firebase/Google API key, the project's Realtime Database URL and the project ID in plaintext (concrete values redacted in this public report and disclosed to Coinbase in R1). Google describes such keys as public by design; the key becomes a lever once every actor holds it. Without server contact or authentication the key enables anonymous quota exhaustion against the Firebase API, push-notification abuse against registered devices, e-mail enumeration through the identity toolkit endpoint, password-reset flooding, and, if the database security rules are permissive, a full Realtime Database read. None of these vectors was exercised; that is R2-only under the standing methodology. The accountability burden for showing that none applies sits with the controller under Art. 5(2).

M1: Datadog Session Replay SDK compiled into a financial application; production activation and field masking not determined (R1 label: H2)

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:R/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.6 - screen-recording capability is present in the binary; whether it records balances, wallet addresses or KYC images was not determined

```
com.datadog.android.sessionreplay.* (312 distinct references, classes7.dex; also
  classes2, 3, 4, 12)
<provider android:name="com.datadog.android.rum.DdRumContentProvider"/>
```

Impact: Datadog's RUM SDK including its Session Replay module is compiled into the app: 312 distinct com.datadog.android.sessionreplay class references in one dex file (classes7) and the DdRumContentProvider declared in the manifest. Presence is a fact. Whether Session Replay is enabled in the production configuration, and whether balances, wallet addresses and KYC document screens are masked through Datadog's privacy-level API, was not determined by this static pass; it requires a runtime capture or a scoped decompile of the initialization call site. R1 labeled this finding HIGH on capability and context. The final report rates it MEDIUM, in line with the severity-consistency discipline that an undetermined runtime behavior does not carry HIGH weight, and keeps the question open: the Article 28 agreement with Datadog for this module is question 2 and remains unanswered.

L1: No network_security_config.xml and no certificate pinning; platform default relied upon

LOW, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N, 3.1 - no pinning means a compromised or coerced system CA could intercept traffic undetected

Impact: No network_security_config.xml exists in the build and no android:networkSecurityConfig attribute or usesCleartextTraffic override is present. With targetSdk 36 the platform default blocks cleartext traffic, the same effective outcome as an explicit base-config. No pin-set is configured, so the app trusts whatever the system CA store trusts for every connection. This is a defensible and common posture for a consumer app and is recorded because of the transaction value the app carries; absence of pinning alone, without a demonstrated interception path, does not constitute demonstrated impact.

Impact Analysis

C1 and C2 are two sides of one decision about advertising data. C1 declares consent as granted for every Consent Mode signal and ships no mechanism to change that state. C2 then opens the Privacy Sandbox surfaces that carry attribution, custom-audience and topics data to every app on the device. Together they describe a build in which a user of a regulated financial application has neither a way to refuse nor a boundary around the resulting data. H1 adds a credential exposure at the infrastructure layer and M1 raises the question of what a screen-recording-capable SDK sees in an application whose screens show balances, wallet addresses and identity documents.

The case is also a contrast study. Coinbase has done the expensive work: a MiCA licence, standard contractual clauses, a Data Privacy Framework certification, a named DPO and a rights dashboard. The cheap work, a consent screen that flips the defaults to denied, is missing from the binary. The three questions put to Coinbase ask only for the documents and the awareness that a company with that maturity should be able to answer in one line.

The Complete Chain: Seven Messages Sent, Eight Responses, Zero Answers

2 July 2026, 10:01 UTC: RFI-IRFOS sends the original disclosure to security@coinbase.com and dpo@coinbase.com, with the DSB, the EDPS and the CNPD in copy, embargo 30 September 2026. Fifteen seconds later the DPO inbox returns an automated acknowledgment.

2 July 2026, 11:05 UTC: security@coinbase.com replies once: 'Thanks for contacting Coinbase Security, we value these reports and collect them in Hacker One', followed by the link to Coinbase's bug-bounty program and the request to submit any vulnerability there. It is the only message security@coinbase.com sends in this correspondence.

2 July 2026, 11:24 UTC: an automatic Gmail emoji reaction (a laughing face) is transmitted from the RFI-IRFOS account to security@coinbase.com with the redirect quoted. It contains no text and is not a written reply; this report records it because it appears in the thread and counts among the messages sent.

2 July 2026, 13:38 UTC: the written reply. RFI-IRFOS answers both addresses jointly, with the DSB, the EDPS and the CNPD in copy, and states that the matter is a GDPR coordinated disclosure addressed to a named Data Protection Officer and not a bug-bounty submission. The DPO inbox again returns the automated acknowledgment. cnpd@cnpd.lu rejects the copy (address not found).

9 August 2026: follow-up, 38 days after the disclosure. The DPO inbox returns the same automated text. cnpd@cnpd.lu and the mistyped edps@europa.eu both reject their copies; the mistyped address was corrected in every later message.

24 August 2026: follow-up, fifteen days after the previous automated acknowledgment. Same automated reply.

31 August 2026: follow-up, seven days later, noting that no human reply had arrived. Same automated reply.

1 September 2026, 17:38 UTC: a Coinbase staff member closes Jira ticket SECURITY-517761 and the service desk sends the closure to RFI-IRFOS only, without any supervisory authority in copy. Status 'Closing, No Outstanding Action', resolution 'Fixed (original response provided 2026-07-02)'. The summary treats the 2 July HackerOne redirect as the resolution; states that six follow-up messages restate the same four findings verbatim and that the same three questions are repeated in three follow-ups 'without modification'; lists the embargo date, the weekly APK comparison, the campaign-size reference and the optional advisory offer in the first message as 'escalating pressure framing'; calls the pattern 'consistent with a disclosure e-pressure/extortion pattern rather than a standard good-faith VDP submission'; and notes that 'independent technical verification of the underlying claims (Consent Mode defaults, AdServices config, Firebase key exposure) is tracked separately and not blocked by this closure'.

1 September 2026, 17:55 UTC: RFI-IRFOS replies to the ticket, with the DSB and the EDPS in copy, that the ticket cannot call the findings fixed and unverified at once, that the embargo date was stated once on 2 July and never moved, that publication was announced as unconditional in the same message that mentioned the optional advisory offer, that the later messages carried no offer, and that the three questions remain open. The DPO inbox answers 16 seconds later with an automated message directing vulnerability reports to HackerOne.

30 September 2026: embargo reached. Correspondence record: 7 messages sent (6 written, 1 emoji reaction), 8 responses (6 automated, 1 bug-bounty redirect, 1 ticket closure), 3 delivery failures, 0 of 3 questions answered.

17 October 2026: this report publishes, 17 days after the embargo and 107 days after the original disclosure. C1 and C2 are treated as unaddressed on the merits; Coinbase has stated that verification is tracked separately and this report records no result of it.

Disclosure Timeline & Outcome

2026-07-02 10:01 Initial disclosure (R1) to security@coinbase.com and dpo@coinbase.com, DSB, EDPS and CNPD in copy. Embargo fixed at 2026-09-30. Automated DPO acknowledgment follows within seconds.

2026-07-02 11:05 Security replies once: bug-bounty redirect to HackerOne.

2026-07-02 11:24 Automatic Gmail emoji reaction from RFI-IRFOS to the redirect. No text.

2026-07-02 13:38 Written reply to security and DPO jointly. Automated DPO acknowledgment. cnpd@cnpd.lu rejects mail (address not found).

2026-08-09 Follow-up. Automated DPO acknowledgment. cnpd@cnpd.lu and the mistyped edps@europa.eu reject their copies.

2026-08-24 Follow-up. Automated DPO acknowledgment.

2026-08-31 Follow-up. Automated DPO acknowledgment.

2026-09-01 Jira ticket SECURITY-517761 closed as Fixed / No Further Action, summary characterizing the correspondence as a pressure pattern. RFI-IRFOS replies the same day. Automated DPO reply.

2026-09-30 Embargo date reached. Correspondence record: 7 sent, 8 responses, 3 delivery failures, 0 questions answered.

2026-10-17 This report published, 17 days after embargo, 107 days after original disclosure. C1 and C2 unaddressed on the merits.

Chinese-Vendor SDK Thesis: Tested, Not Confirmed

Per standing methodology every audit tests for Chinese-origin SDKs regardless of expectation. A broad substring search returned apparent hits that were each run down individually. 'mbridge' matched inside 'Cambridge' (a timezone name string), not the Mintegral SDK, and no com/mbridge or Mintegral path exists in the unpacked APK. 'alibaba' matched inside the bundled public-suffix list of top-level domain names, not an SDK, and no com/alibaba or com/aliyun path exists. The one genuine Chinese-origin component, com.tencent.mmkv, is Tencent's open-source local key-value storage library, which has no network capability of its own and is used by thousands of apps worldwide; it is noted and not scored. No Mintegral, ByteDance, Pangle, Baidu, Umeng, Aliyun, Tencent Cloud, JPush, Xiaomi push or Getui strings or classpaths were found in the manifest, resources or any of the 12 dex string dumps. The thesis is not confirmed for this build, and the negative result is part of the public record.

What Coinbase Got Right

Onfido's KYC components are process-isolated: a dedicated :onfido_process, all providers exported=false, activation only on an explicit user-initiated verification and not at cold start. ACCESS_BACKGROUND_LOCATION is not requested, so location access is foreground-only. allowBackup=false and extractNativeLibs=false. DETECT_SCREEN_CAPTURE is present as a defense against overlay-style banking trojans. Cleartext HTTP is blocked through the platform default. The camera and microphone permission rationale strings map verbatim to the Onfido liveness flow. Coinbase Luxembourg S.A. holds a full MiCA licence with EU-wide passporting, a more engaged regulatory relationship than the exit-only posture seen elsewhere in this audit series. A DPO contact (dpo@coinbase.com) and a self-service privacy rights dashboard exist and function as rights-request channels, which several apps in this series lack entirely.

Data Protection Article by Article

Art. 4(11), Art. 6 and Art. 7 GDPR: C1 sets every Consent Mode default to granted and ships no mechanism to deny. Consent that is permanently preset cannot be freely given, specific, informed and unambiguous, and consent collected later cannot retroactively authorize processing that started at process creation. Question 1 asked whether Coinbase's security and privacy team is aware of this.

Art. 5(1)(a) GDPR: lawfulness, fairness and transparency are implicated by a build that processes advertising signals under a preset yes.

Art. 25 GDPR: C2 and C1 are data-protection-by-default decisions. The default of the Privacy Sandbox access policy is the most permissive one and the default of every Consent Mode signal is granted.

Art. 5(1)(f) and Art. 32 GDPR: C2's cross-app access and H1's hardcoded key are integrity and confidentiality questions at the technical-measure level.

Art. 28 GDPR: whether a documented processing agreement with Datadog covers the Session Replay module is question 2. It remains unanswered.

Art. 5(2) GDPR: for H1 the burden of showing that anonymous quota abuse, enumeration and database reads are not possible rests with the controller.

Art. 33 GDPR: if any of the findings qualifies as a personal data breach the 72-hour clock runs from awareness. The supervisory authority copies have had full visibility since 2 July 2026.

Art. 35 GDPR: biometric KYC data (facial images and video liveness through Onfido, Art. 9 special-category data) combined with a session-replay-capable SDK in the same application is a high-risk combination for which a DPIA is expected; whether it exists and has reached the DPO was raised in R1 and remains unanswered.

Regulatory Landscape & Fine Exposure

Coinbase's EU crypto-asset activity is authorized through Coinbase Luxembourg S.A. under the CSSF's MiCA regime, and the Luxembourg CNPD is the data protection authority for a Luxembourg establishment. RFI-IRFOS copied the CNPD, but the published address rejected mail on both attempts, so this report cannot assume the CNPD received the correspondence. The Austrian DSB, as the initiating authority, and the EDPS received every message from the first. Any member-state authority where affected users reside may independently assert competence.

Art. 83(5) GDPR: fines up to EUR 20,000,000 or 4% of worldwide annual turnover apply to violations of Art. 5, 6, 7 and 9. C1 implicates this tier directly.

Art. 83(4) GDPR: fines up to EUR 10,000,000 or 2% of worldwide annual turnover apply to violations of Art. 25, 28, 32 and 35. C2, H1 and M1 implicate this tier.

This report states exposure categories; it does not predict any authority's decision.

Indicators of Compromise

All findings derive from static analysis of com.coinbase.android v14.24.32 as published on Google Play, analyzed 2026-07-02. base.apk SHA-256: b0a7217dd4ca1309fe09c01f8928c0bd80655230badd5bdb2a81c27759c3e6cb. Files of interest: AndroidManifest.xml (Consent Mode meta-data, FirebaseInitProvider), res/xml/ad_services_config.xml, res/values/strings.xml (Firebase values, redacted here), classes7.dex (Datadog Session Replay). No Coinbase servers, accounts or production infrastructure were probed or accessed.

Residual Risk & Recommendations

C1: ship Consent Mode defaults as denied and update them to granted only after an affirmative choice in a consent screen that appears before FirebaseInitProvider-driven collection; add a consent-management mechanism; document the Art. 6 basis for anything collected before that choice.

C2: set allowAllToAccess to false or list only the specific SDKs and apps that need attribution, custom-audience or topics access; request only the AdServices permissions that a documented measurement purpose requires.

H1: rotate the exposed key, restrict it to the app's package name and signing certificate in the Google Cloud console, verify that the Realtime Database security rules deny unauthenticated reads and writes, and remove the values from version-controlled resource files.

M1: confirm whether Session Replay is enabled in production; if it is, apply the strictest masking privacy level to balance, wallet and KYC screens and document the Art. 28 agreement with Datadog; if it is not, remove the module.

L1: evaluate certificate pinning for the trading and KYC endpoints given the transaction value.

Process-level: a DPO inbox that returns the same automated text six times and a Security inbox that returns one redirect need an internal route to a person who can read a coordinated disclosure addressed to the DPO. A ticket that closes a finding as fixed while stating that verification is tracked separately should record the verification result.

Open R2 items for RFI-IRFOS: cold-start network capture to confirm live transmission before any consent action, live test of the Firebase key against the five documented vectors, cross-app AdServices access test, scoped decompile of the Datadog Session Replay initialization call site, and a primary-source review of coinbase.com/legal/privacy from a non-automated context.

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 com.coinbase.android as published on Google Play, analyzed 2026-07-02, using publicly available tools (apktool, aapt2, string extraction). No Coinbase servers, accounts or production infrastructure were probed or accessed. Statements about Coinbase's privacy policy rest on search-indexed excerpts and public press material because the policy pages returned HTTP 403 to automated fetch. Technical evidence is archived under chain of custody and will be provided to the competent supervisory authority 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 CB-2026-R1-001.