



Security & Privacy Disclosure, Final Report

Perplexity ([ai.perplexity.app.android](https://ai.perplexity.app/android)) v2.91.1

An Android search app that ships as an operating-system-level personal assistant: SMS, Gmail, contacts, calendar and notification access, a lock-screen mode its own strings warn about, Firebase and a first-party tracker started before any consent screen, and a real-time voice pipeline that reaches four outside AI vendors

PUBLIC DISCLOSURE, 17 OCTOBER 2026. EMBARGO REACHED 30 SEPTEMBER 2026, WRITTEN POSITION RECEIVED 29 SEPTEMBER, NO YES OR NO ANSWER TO ANY OF THE THREE QUESTIONS

Target	Perplexity AI, Inc. (United States). Art. 27 representative and Data Protection Officer per Perplexity's privacy notice of 8 July 2026 and its message of 29 September 2026: VeraSafe. Contact mailboxes used: privacy@perplexity.ai and support@perplexity.ai
Package	ai.perplexity.app.android (versionCode 260623), minSdk 32, targetSdk 36
Platform	Android, static analysis (base.apk 94,147,802 bytes plus split_config.arm64_v8a.apk 60,249,356 bytes; four classes*.dex files, about 36 MB)
Initial Disclosure (R1)	2026-07-02 (REF PPLX-2026-R1-001)
Disclosure / Embargo Date	2026-09-30
Report Published	2026-10-17
Overall Severity	HIGH
Findings	6 (3 High, 2 Medium, 1 Low) plus 1 negative result on Chinese and Russian SDKs
Correspondence	16 messages sent by RFI-IRFOS between 2 July and 29 September 2026 under REF PPLX-2026-R1-001: 12 in the main thread to privacy@perplexity.ai and support@perplexity.ai (2 July, 6 July, 17 July, 27 July, 5 August, 15 August, 18 August, 21 August, 24 August, 28 August, 10 September, 29 September), one to privacy@perplexity.ai and office@prighter.com (22 August), two to Prighter support and its CEO (25 August), and one to experts@verasafe.com and privacy@perplexity.ai (25 August). The Austrian DSB and the EDPS were in copy on every message. Perplexity-side systems sent 26 messages in the main thread: 6 mailbox-not-monitored autoreplies, 10 automated acknowledgments or hand-offs, 4 identical automated ticket-closure warnings, 5 support replies that state no confirmed internal information (27 July, 15 August, 18 August, 21 August, and a 10 September holding message from a self-described human agent) and 1 written position statement on 29 September. Prighter sent 2 messages.
Authorities CC'd	Österreichische Datenschutzbehörde (DSB), Austria; European Data Protection Supervisor (EDPS). No delivery failure was recorded for these addresses on this case.
SHA-256 (base APK)	c0cb2029e2cd688ff5ac2ca28a037b5de6964496195eb5a74351cea43f753eb4

Contents

1	Executive Summary	4
2	Subject & Operator Context	5
3	Engagement Summary	5
4	Findings	6
4.1	H1: Operating-system-level assistant surface: SMS, contacts, calendar, phone and a system-wide notification listener, with a self-disclosed lock-screen risk	6
4.2	H2: Firebase and a first-party tracker initialize at process creation, before any consent screen; no consent management implementation in the binary	7
4.3	H3: Real-time voice feature reaches four outside AI vendors (OpenAI, Google Gemini, ElevenLabs, Soniox) through backend-issued provider keys	8
4.4	M1: Four API keys and tokens in plaintext in strings.xml: two Google keys, a Mapbox token and an Eppo token	9
4.5	M2: Singular attribution SDK and advertising-identifier permissions in an application with no ad-serving SDK	10
4.6	L1: No age-assurance mechanism of any kind in the resources	10
5	Impact Analysis	11
6	The Complete Chain: 16 Messages Sent, 28 Replies Received, Questions Not Answered Yes or No	11
7	Disclosure Timeline & Outcome	12
8	Perplexity's Written Position of 29 September 2026	13
9	What Perplexity Got Right	13
10	Data Protection Article by Article	14
11	Regulatory Landscape & Fine Exposure	14
12	Indicators of Compromise	15
13	Residual Risk & Recommendations	15

Executive Summary

Perplexity's Android application (ai.perplexity.app.android v2.91.1) was analyzed on 2 July 2026 with apktool, an independent aapt2 dump and string extraction across all four dex files, plus a full native library inventory. The analysis started without a thesis. It found an application that ships as an operating-system-level personal assistant, and the report records three HIGH findings, two MEDIUM findings and one LOW finding.

H1: the manifest requests READ_SMS, SEND_SMS, READ_CONTACTS, READ_CALENDAR, WRITE_CALENDAR, CALL_PHONE and ANSWER_PHONE_CALLS and declares a Notification-ListenerService that can read the content of every notification from every app once the user grants notification access. The app's own string resource states that with lock-screen actions enabled, anyone with physical access to the phone can use the assistant to send messages, set alarms and view personal information without unlocking the device. H2: FirebaseInitProvider and the first-party AppStartTrackerProvider are initialized at process creation, before any Activity and therefore before any consent screen, and no consent management implementation exists in the binary. H3: the real-time voice feature contains code that connects to OpenAI (a hardcoded realtime WebSocket URL), Google Gemini, ElevenLabs and Soniox, with provider keys issued by Perplexity's backend through named REST endpoints and a native WebRTC library present.

Perplexity's posture contains real strengths, recorded below: a per-capability connector model instead of one blanket consent button, a plain-language warning about the lock-screen risk, an empty network security config that leaves the platform defaults in force, no background location, no Chinese or Russian SDK in a deliberate check, and an Article 27 representative and Data Protection Officer that Perplexity's own messages name as VeraSafe. The R1 message named Prighter Group as the representative. That was outdated: Perplexity's privacy notice of 8 July 2026 names VeraSafe, and RFI-IRFOS corrected its record with Prighter on 25 August 2026.

RFI-IRFOS put three yes or no questions to Perplexity on 2 July 2026: whether a documented Art. 35 DPIA exists for the combination of lock-screen actions, notification listener and the Messages, Gmail and Contacts connectors; whether OpenAI, Google Gemini, ElevenLabs and Soniox are named as sub-processors for EU users with Art. 28 contracts and Art. 46 mechanisms; and whether the Austrian DSB knows of the change of Art. 27 representative. The questions were repeated and, from 10 September, re-worded. Perplexity's support channel answered on 27 July, 15 August, 18 August and 21 August that it holds no confirmed internal information on these points and linked public pages. On 29 September 2026, one day before the embargo, Perplexity sent a written position statement. It disputes that a lock-screen assistant is a risk, describes AppStartTracker as first-party code that measures app start time and Firebase as strictly necessary diagnostics, and states that VeraSafe is the Art. 27 representative and DPO and has passed RFI-IRFOS's message to the Legal and GRC teams. It does not state whether a DPIA exists, does not name OpenAI, Google Gemini, ElevenLabs or Soniox, and does not state whether the DSB was informed of the representative changes. The embargo ended on 30 September 2026 without a yes or no answer to any question.

ID	Severity	Title
H1	HIGH	Operating-system-level assistant surface: SMS, contacts, calendar, phone and a system-wide notification listener, with a self-disclosed lock-screen risk

ID	Severity	Title
H2	HIGH	Firebase and a first-party tracker initialize at process creation, before any consent screen; no consent management implementation in the binary
H3	HIGH	Real-time voice feature reaches four outside AI vendors (OpenAI, Google Gemini, ElevenLabs, Soniox) through backend-issued provider keys
M1	MEDIUM	Four API keys and tokens in plaintext in strings.xml: two Google keys, a Mapbox token and an Eppo token
M2	MEDIUM	Singular attribution SDK and advertising-identifier permissions in an application with no ad-serving SDK
L1	LOW	No age-assurance mechanism of any kind in the resources

Subject & Operator Context

Perplexity AI, Inc. is a United States company that publishes the Perplexity answer engine and assistant for Android as `ai.perplexity.app.android`. The binary reports versionCode 260623 with targetSdk 36 and requests the newer Android App Functions permissions (EX ECUTE_APP_FUNCTIONS and READ_ASSISTANT_APP_SEARCH_DATA among them), which places it in the class of apps that position themselves as the system assistant. RFI-IRFOS identified no EU main establishment, so the Austrian Datenschutzbehörde acted as the initiating authority under RFI-IRFOS's standing practice for Austrian-initiated audits. Perplexity's Art. 27 representative and DPO is VeraSafe according to Perplexity's privacy notice dated 8 July 2026 and its own message of 29 September 2026. Operator facts were taken from the binary and from public pages; the privacy policy and trust center pages returned bot-protection or JavaScript shells to automated fetch, so statements about them rely on search-indexed excerpts and on Perplexity's own replies.

Engagement Summary

RFI-IRFOS analyzed `ai.perplexity.app.android` v2.91.1 on 2 July 2026 using apktool (manifest, resources and strings without baksmali, a memory-safe pass for an application of this size), raw string extraction run sequentially across all four `classes*.dex` files, an independent aapt2 permission and version dump, and a full inventory of the arm64 native libraries. No Perplexity server, account or production system was accessed and no key found in the binary was used. Findings are classified as observed fact, where the artifact itself shows the behavior, or inference, where a runtime capture (R2) would be needed. Severity labels follow the RFI-IRFOS blast-radius method: the CVSS v4.0 base score is shown in each finding box and a label above the score band is explained in the finding text. CVSS 4.0 scores in this report were assigned from the standard vector pairs used across the 2026 series and were not produced by a calculator.

Findings

H1: Operating-system-level assistant surface: SMS, contacts, calendar, phone and a system-wide notification listener, with a self-disclosed lock-screen risk

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 - dangerous permission set plus NotificationListenerService, lock-screen actions disclosed by the app itself

```
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.CALL_PHONE"/>
<uses-permission android:name="android.permission.SEND_SMS"/>
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.READ_CALENDAR"/>
<uses-permission android:name="android.permission.WRITE_CALENDAR"/>
<uses-permission android:name="android.permission.ANSWER_PHONE_CALLS"/>
<service android:exported="false" android:name="ai.perplexity.app.android.assistant.
    action.NotificationListener"
    android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE">
    <intent-filter><action android:name="android.service.notification.
        NotificationListenerService"/></intent-filter>
</service>
```

```
allow_assistant_actions_on_lock_screen_description = When enabled, anyone with
    physical access to your phone can use the assistant to send messages, set alarms,
    and view personal information without unlocking your device.
assistant_app_connectors_messages_description = Allow the assistant to read your
    messages
assistant_app_connectors_gmail_description = Allow the assistant to read your Gmail
    emails
assistant_app_connectors_contacts_description = Allow the assistant to read your
    contacts
assistant_app_connectors_calendar_description = Allow the assistant to read, create,
    and modify events in your calendar
assistant_app_connectors_phone_description = Allow the assistant to make phone calls
```

Impact: The manifest requests READ_SMS, SEND_SMS, READ_CONTACTS, READ_CALENDAR, WRITE_CALENDAR, CALL_PHONE and ANSWER_PHONE_CALLS next to CAMERA, RECORD_AUDIO and fine and coarse location, and declares ai.perplexity.app.android.assistant.action.NotificationListener bound to BIND_NOTIFICATION_LISTENER_SERVICE. Once the user grants the separate Notification access setting, that class can read the title, text and extras of every notification posted by every app on the device. The app's string resources describe the intended use in its own words: the assistant reads messages, reads Gmail, reads contacts and creates and modifies calendar events, and the lock-screen string states: 'When enabled, anyone with physical access to your phone can use the assistant to send messages, set alarms, and view personal information without unlocking your device.' The connector strings are named per capability (Messages, Gmail, Contacts, Calendar, Phone), which indicates separate toggles and is recorded as a strength. Observed fact:

the permissions, the service declaration and the strings exist as quoted. Not observed: a runtime trace of what the notification listener captures, which requires a controlled device test. RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.1 to HIGH because the combination reaches message, mail, contact, calendar and cross-app notification content in one assistant for every user who enables the connectors, and the app itself names the physical-access consequence, a scope the CVSS technical vector does not capture. On 29 September 2026 Perplexity stated that it does not agree with the characterization of the lock-screen assistant as a risk, that the feature uses Android operating-system APIs, and that it must be affirmatively enabled when the user sets Perplexity as the default assistant. Perplexity did not state whether a DPIA exists for the combination.

H2: Firebase and a first-party tracker initialize at process creation, before any consent screen; no consent management implementation in the binary

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 - two ContentProviders start before the first Activity and no CMP or TCF user interface exists

```
<provider android:authorities="ai.perplexity.app.android.appstarttracker" android:
  exported="false"
  android:initOrder="101" android:name="ai.perplexity.app.android.tracking.
  AppStartTrackerProvider"/>
<provider android:authorities="ai.perplexity.app.android.firebaseinitprovider" android
  :directBootAware="true"
  android:exported="false" android:initOrder="100" android:name="com.google.firebase.
  provider.FirebaseInitProvider"/>
```

Impact: com.google.firebase.provider.FirebaseInitProvider (initOrder 100, directBootAware) and ai.perplexity.app.android.tracking.AppStartTrackerProvider (initOrder 101) are declared as ContentProviders. Android runs a provider's onCreate during application process creation, before the first Activity, so both start before any consent interface can render; exported=false limits access by other apps and does not delay initialization. A targeted search for OneTrust, Didomi, Usercentrics and IAB TCF implementations across all four dex string tables found none. The IABTCF strings that exist are shared-preference keys read by RevenueCat's attribution code. The manifest also carries the Firebase Analytics, Crashlytics, Performance Monitoring, Remote Config and Cloud Messaging component set. Observed fact: both providers initialize before any consent screen and no consent management implementation was found. Not observed: what either provider's onCreate collects or transmits in that window, which requires a cold-start network capture. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the structure applies to every launch of an application that also holds the H1 permission set, so valid consent cannot precede the first processing. On 29 September 2026 Perplexity stated that AppStartTracker is its own code that reports how long the app takes to open, that it is not designed to transmit personal data or give data to third parties, and that it regards Firebase as strictly necessary for crash and stability diagnostics. These statements are recorded as Perplexity's position; the manifest shows more Firebase components than crash diagnostics, and neither statement has been verified at runtime.

H3: Real-time voice feature reaches four outside AI vendors (OpenAI, Google Gemini, ElevenLabs, Soniox) through backend-issued provider keys

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 - hardcoded realtime WebSocket URL, Gemini and Soniox key endpoints and a native WebRTC library

```
wss://api.openai.com/v1/realtime?intent=transcription
ai.perplexity.app.android.voice2voice.impl.realtime.gemini.GeminiBlob
ai.perplexity.app.android.voice2voice.impl.realtime.model.config.GeminiConfig
ai.perplexity.app.android.voice2voice.impl.realtime.model.config.OpenAIConfig
ai.perplexity.app.android.voice2voice.impl.realtime.model.config.RealtimeVoiceProvider
ai.perplexity.multimodal.tts.api.config.ElevenLabsVoice$Custom
/rest/realtime/v1/transcription/gemini-api-key
/rest/realtime/v1/transcription/soniox-api-key
lib/arm64-v8a/libjingle_peerconnection_so.so 11278608 bytes
```

Impact: The dex strings contain `wss://api.openai.com/v1/realtime?intent=transcription`, a Kotlin package tree `ai.perplexity.app.android.voice2voice.impl.realtime.gemini.*` with `GeminiConfig` and `OpenAIConfig` beside a `RealtimeVoiceProvider` type, the `ElevenLabsVoice` text-to-speech configuration, and the backend paths `/rest/realtime/v1/transcription/gemini-api-key` and `/rest/realtime/v1/transcription/soniox-api-key`. The arm64 split ships `libjingle_peerconnection_so.so` (11,278,608 bytes), the WebRTC peer-connection library. The pattern of a backend that issues per-provider keys to the client indicates a connection from the device to each provider. All four named vendors are US-headquartered, so Art. 28 and Art. 44 to 46 apply to every one of them. Perplexity's trust center subprocessor page is a JavaScript-rendered application that returned an empty shell to automated fetch, which is why question 2 asked for a yes or no. Observed fact: the code, endpoints and library exist. Not observed: network capture of a voice session showing where audio goes. RFI-IRFOS blast-radius escalation: raised from MEDIUM/4.6 to HIGH because voice audio is personal data from every user who opens the voice feature and the chain involves four outside processors in a third country. On 27 July, 15 August and 18 August 2026 Perplexity's support replies pointed to the trust center and stated that they hold no confirmed answer on whether the four vendors are listed for EU users. The 29 September statement does not name any of the four vendors.

M1: Four API keys and tokens in plaintext in strings.xml: two Google keys, a Mapbox token and an Eppo token

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N, 4.5 - credentials shipped in the public APK, restriction state not verifiable from outside

```
eppo_access_token = [REDACTED IN PUBLIC REPORT -- disclosed privately to Perplexity in R1]
google_api_key = [REDACTED IN PUBLIC REPORT -- disclosed privately to Perplexity in R1]
mapbox_access_token = [REDACTED IN PUBLIC REPORT -- disclosed privately to Perplexity in R1]
places_api_key = [REDACTED IN PUBLIC REPORT -- disclosed privately to Perplexity in R1]
```

Impact: res/values/strings.xml holds google_api_key and places_api_key (Google Cloud keys), mapbox_access_token (a public pk. token tied to the Mapbox Maps and Geofencing integration) and eppo_access_token (the feature-flag platform Eppo). All four sit in the shipped, publicly downloadable APK and were extracted with apktool and no privileged access. Google API keys and Mapbox public tokens are designed to be embedded and are normally limited by package, signing certificate or referrer restrictions in the vendor console. Whether those restrictions are configured sits with the operator, and RFI-IRFOS did not invoke any key. The exact values are withheld from this public report and were given to Perplexity in R1: [REDACTED IN PUBLIC REPORT – disclosed privately to Perplexity in R1].

M2: Singular attribution SDK and advertising-identifier permissions in an application with no ad-serving SDK

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 - AD_ID and AdServices attribution permissions feed a full attribution SDK

```
<uses-permission android:name="com.google.android.gms.permission.AD_ID"/>
<uses-permission android:name="android.permission.ACCESS_AD SERVICES_ATTRIBUTION"/>
<uses-permission android:name="android.permission.ACCESS_AD SERVICES_AD_ID"/>
<uses-permission android:name="com.singular.preinstall.READ_PERMISSION_SINGULAR"/>
```

Impact: The manifest requests com.google.android.gms.permission.AD_ID, ACCESS_AD SERVICES_ATTRIBUTION, ACCESS_AD SERVICES_AD_ID and the Singular preinstall read permission, and declares a singular-perplexity deep-link scheme. The dex strings show the Singular SDK in full, including its ApiGDPRConsent and ApiGDPRUnder13 classes, so the vendor supports consent-gated start. A targeted check found no AppsFlyer, Mixpanel or Ad-Mob ad-serving classpath; the AppsFlyer and Mixpanel strings that matched are RevenueCat passthrough setters and an admob_app_id column in Firebase Analytics' own local database. Observed fact: Singular is integrated and the identifier permissions are requested. Not observed: whether Perplexity's start-up code calls the Singular consent API before collection begins, which needs a trace of Application.onCreate.

L1: No age-assurance mechanism of any kind in the resources

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 date-of-birth prompt, no age gate

```
error_message_parental_control_restricted = That content is blocked
```

Impact: A targeted search of strings.xml for age, birthday, date-of-birth and parental terms found no age gate. The only related string, error_message_parental_control_restricted ('That content is blocked'), is a content-availability message and no gate for the application itself. This is recorded at LOW for a general-purpose application whose stated audience is not children.

Impact Analysis

H1, H2 and H3 describe one product decision from three directions. H1 sets the reach of the assistant: message, mail, contact, calendar and notification content, with a lock-screen mode the app itself warns about. H2 shows that two components start before the user can decide anything. H3 shows that spoken input leaves through a chain of four outside AI vendors. A user who enables the assistant, opens the voice feature and never sees a consent screen has no point at which a choice preceded the processing. M1 and M2 add credentials and an attribution identifier to the same picture, and L1 notes that nothing restricts who installs it. The negative result is as important: a deliberate search found no Chinese or Russian SDK.

The Complete Chain: 16 Messages Sent, 28 Replies Received, Questions Not Answered Yes or No

R1 on 2 July 2026 asked three yes or no questions: (1) a documented Art. 35 DPIA for the combination of lock-screen actions, notification listener and the Messages, Gmail and Contacts connectors; (2) OpenAI, Google Gemini, ElevenLabs and Soniox named as sub-processors for EU users with Art. 28 contracts and Art. 46 mechanisms; (3) the Austrian DSB's knowledge of the change of Art. 27 representative from DataRep to Prighter. From 15 August the follow-ups put the questions in shorter form, and the 10 September message re-worded them: lock-screen access documented as a standalone risk, a DPIA for the pre-consent providers, and the representative consistently reflected after the change to VeraSafe. The 29 September answer from Perplexity responds to that 10 September wording. Both sets of questions appear in the correspondence and this report records both.

Perplexity-side responses, main thread: 2 July, three messages within four minutes (a mailbox-not-monitored autoreply, an automated acknowledgment and an automated hand-off stating the chat had moved into areas it could not handle); 6 July, two (autoreply and hand-off); 17 July, two automated confirmations; 27 July, three (autoreply, acknowledgment, and a reply from privacy@perplexity.ai stating that it holds no yes or no confirmation on the three points and linking the trust center, sub-processor notification page, DPA, Data Privacy Framework list and privacy policy); 5 August, three automated messages; 15 August, an automated acknowledgment and a support reply listing the same public pages and stating that it holds no confirmed internal information on the lock-screen risk, the DPIA or the update of the representative; 18 August, an automated warning that the ticket would be closed for lack of response, followed by a support reply stating the warning was 'in diesem Kontext nicht passend' and repeating that it could not confirm the three points; 21 August, the same closure warning again, followed by an apology; 24 August, the closure warning a third time and an acknowledgment; 27 August, the closure warning a fourth time; 10 September, a message from a self-described human agent (signed 'Jennifer Perplexity Support') stating that the case is under review, that the ticket stays open, and apologizing for the closure messages that fired incorrectly; 29 September, 04:38 UTC, the written position statement described in the findings.

Representative thread: on 22 August RFI-IRFOS wrote to privacy@perplexity.ai and office@prighter.com. On 25 August Prighter support replied that Prighter Group is not acting as Perplexity's Art. 27 representative, and Prighter's CEO, an attorney, replied that Prighter found no mention of Prighter or iuro in Perplexity's privacy policy and asked for a screenshot and URL. RFI-IRFOS had quoted a third-party mirror dated November 2025; it then pulled Perplexity's privacy notice (last updated 8 July 2026), found VeraSafe named as Art. 27

representative and DPO, and told Prighter that its denial was correct and that RFI-IRFOS's source was out of date. On 25 August RFI-IRFOS wrote to experts@verasafe.com and privacy@perplexity.ai. VeraSafe sent no direct reply; Perplexity's 29 September statement says VeraSafe received the message and brought it to the Legal and GRC teams.

RFI-IRFOS's reply of 29 September, 06:35 UTC, stated that the three questions remained unanswered in yes or no form and that the embargo would end on 30 September.

Disclosure Timeline & Outcome

2026-07-02 15:00 Initial disclosure (R1) to privacy@perplexity.ai, support@perplexity.ai, DSB and EDPS in copy. Embargo fixed at 2026-09-30. Automated replies follow within four minutes.

2026-07-06 Follow-up. Automated replies.

2026-07-17 Follow-up. Automated confirmations.

2026-07-27 Follow-up. privacy@perplexity.ai replies that it has no yes or no confirmation and links public pages.

2026-08-05 Follow-up. Automated messages.

2026-08-15 Follow-up. Support replies with public links and no confirmed internal information.

2026-08-18 Follow-up. Automated ticket-closure warning, then a support reply calling the warning inappropriate for the context.

2026-08-21 Follow-up. The same closure warning, then an apology.

2026-08-22 Message to Perplexity privacy and to Prighter office.

2026-08-24 Follow-up. The closure warning a third time, then an acknowledgment.

2026-08-25 Prighter denies being the representative; RFI-IRFOS corrects its record and writes to VeraSafe.

2026-08-27 The closure warning a fourth time.

2026-08-28 Follow-up.

2026-09-10 Support message from a self-described human agent: case under review.

2026-09-29 Perplexity written position statement (04:38 UTC). RFI-IRFOS reply (06:35 UTC).

2026-09-30 Embargo date reached. Correspondence record: 16 sent, 28 received, 0 yes or no answers to the three questions.

2026-10-17 This report published, 17 days after embargo, 107 days after original disclosure.

Perplexity's Written Position of 29 September 2026

Perplexity answered three numbered points. Point 1: the privacy notice informs data subjects of the type of information processed, the legal purpose and the rights; Perplexity does not agree with the characterization of a lock-screen assistant as a risk; the lock-screen assistant is a design feature that uses Android operating-system APIs to read text messages or calendar information without unlocking the device; the user must affirmatively enable it when setting Perplexity as the default assistant; it is expected user functionality enabled by Android and Google. Point 2: AppStartTracker is not a third-party technology, it is Perplexity-created code that reports how long the app takes to open, intended to ensure correct operation and not designed to transmit personal data or provide data to third parties; Firebase produces diagnostic data that help detect and fix crashes; Perplexity views these functions as strictly necessary. Point 3: VeraSafe has been appointed Art. 27 representative and DPO, the privacy notice has been updated, and VeraSafe passed RFI-IRFOS's communication to the Legal and GRC teams.

What the statement leaves out: it does not say whether a DPIA exists for the assistant surface; it does not name OpenAI, Google Gemini, ElevenLabs or Soniox or state whether they are listed as sub-processors for EU users; it does not state whether the Austrian DSB was told about the representative changes; it does not address the pre-consent timing of Firebase Analytics, Remote Config and Cloud Messaging beyond calling diagnostic functions necessary. RFI-IRFOS records the statement as Perplexity's position and has not verified the AppStartTracker description at runtime. The 29 September statement is the only message in the correspondence that addresses the substance of a finding.

What Perplexity Got Right

A per-capability connector model: Messages, Gmail, Contacts, Calendar and Phone each carry their own named description, which indicates separate toggles and is better than a single blanket consent button.

Honest wording about a real risk: the lock-screen string tells the user what can happen if the feature is enabled.

An empty network security config, so the platform defaults for targetSdk 36 apply (cleartext disabled, system certificate authorities only), and no hardcoded http endpoint of consequence.

No ACCESS_BACKGROUND_LOCATION, no READ_PHONE_STATE, no BLUETOOTH_SCAN, no BODY_SENSORS and no ACTIVITY_RECOGNITION, each confirmed absent by direct search.

No Chinese or Russian SDK: Tencent, ByteDance, Alibaba, Baidu, Mintegral, JPush, Getui, Xiaomi push, VK, myTarget and Yandex classpaths were searched across all four dex string tables. The initial hits resolved to a top-level-domain regex list in a URL library and Stripe's WeChat Pay payment module.

Industry-standard payment and subscription infrastructure (Stripe, RevenueCat, Google Play Billing), and camera and Bluetooth declared as optional features.

An Art. 27 representative and DPO that Perplexity names publicly and confirmed in writing. The R1 message named Prighter as the representative. That was outdated by the time of publication; this report names VeraSafe.

Data Protection Article by Article

Art. 5(1)(c) and Art. 35 GDPR: the combination in H1 is the kind of large-scale processing for which a DPIA is considered. Question 1 asked whether one exists for the combination. Perplexity's replies did not say.

Art. 6 and Art. 7 GDPR: H2 shows that processing components start before any consent interface. Valid consent cannot precede processing that begins at process creation.

Art. 13(1)(e) and Art. 14(1)(e) GDPR: recipients or categories of recipients. H3 names four candidate recipients of voice data. Question 2 asked whether they are listed for EU users.

Art. 28, Art. 44 and Art. 46 GDPR: each of the four vendors is US-headquartered, so a processor contract and a transfer mechanism are required for each. Perplexity's replies point to a DPA, the sub-processor notification page and the Data Privacy Framework list and name none of the four.

Art. 27 GDPR: Perplexity's privacy notice of 8 July 2026 names VeraSafe as representative. Question 3 asked about the authority's knowledge of the change. It remains unanswered.

Art. 5(2) GDPR: for M1 the burden of showing that the embedded keys carry no abuse risk sits with the controller.

Art. 8 GDPR: L1 records the absence of any age gate.

Regulatory Landscape & Fine Exposure

No EU main establishment of Perplexity was identified. The Art. 27 representative is a contact point and creates no Art. 56 lead authority, so the Austrian Datenschutzbehörde acted as the initiating authority. The DSB and the EDPS received every message in the main thread. 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, 9 and 44 to 46. H2 and H3 implicate this tier.

Art. 83(4) GDPR: fines up to EUR 10,000,000 or 2% of worldwide annual turnover apply to violations of Art. 8, 25, 27, 28, 32 and 35. H1, M1 and L1 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 ai.perplexity.app.android v2.91.1 as published on Google Play, analyzed 2026-07-02. base.apk SHA-256: c0cb2029e2cd688ff5ac2ca28a037b5de6964496195eb5a74351cea43f753eb4. split_config.arm64_v8a.apk SHA-256: a5ad8ffded60ca64385bba0b8ec8ac11e8bd00885e7c9ae75cb88cb0d4e100cb. Files of interest: AndroidManifest.xml (permissions, NotificationListener, providers), res/values/strings.xml (assistant strings, credential strings withheld here), classes2.dex (realtime voice classes and WebSocket URL), lib/arm64-v8a/libjingle_peerconnection_so.so. No Perplexity servers, accounts or production infrastructure were probed or accessed.

Residual Risk & Recommendations

H1: document an Art. 35 DPIA for the lock-screen, notification-listener and connector combination and publish its existence; offer lock-screen actions as an off-by-default choice with a confirmation step before any message is sent or personal information is read.

H2: move any collection that is not strictly necessary behind the consent decision, set Firebase Analytics, Performance Monitoring and Remote Config to start after consent, and document the legal basis for what runs before it.

H3: publish OpenAI, Google Gemini, ElevenLabs and Soniox in a sub-processor list that is retrievable without JavaScript, with Art. 28 contracts and Art. 46 mechanisms for each.

M1: rotate the four credentials, restrict the Google keys to the package name and signing certificate, restrict the Mapbox token by scope, and remove the values from version-controlled resource files.

M2: call the Singular consent API before the SDK starts and document the purpose of the attribution identifiers in a subscription product.

L1: decide and document whether an age gate is needed.

Process-level: a privacy mailbox that states it is not monitored, an automated closure warning that fired four times after a support reply called it inappropriate, and a change of Art. 27 representative that surfaced only through a third-party correction, all point to the same gap: no route from the inbox to a person who can read a coordinated disclosure. The 29 September statement shows that route exists once escalation happens.

Open R2 items for RFI-IRFOS: network capture of a voice session; cold-start capture of the pre-consent window; a trace of the Singular consent call; a controlled test of the notification listener and lock-screen actions; a JavaScript-executing fetch of the trust center sub-processor list. A later app version is not covered by this report.

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

ai.perplexity.app.android as published on Google Play, analyzed 2026-07-02, using publicly available tools (apktool, aapt2, string extraction). No Perplexity servers, accounts or production systems were accessed and no embedded key was used. Statements about Perplexity's privacy notice and trust center rest on search-indexed excerpts and on Perplexity's own messages because those pages returned bot-protection or JavaScript shells to automated fetch. Technical evidence is archived un-

der 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 PPLX-2026-R1-001.