



Security & Privacy Disclosure, Final Report

Amazon Shopping for Android
(com.amazon.mShop.android.shopping)

Blood glucose and cervical mucus records, an undisclosed 1,817-class EMV payment terminal, and an Alexa microphone wired into shopping navigation shipped unanswered through a 91-day disclosure that Amazon's own publication of a companion case never covered

PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 19 SEPTEMBER 2026, SIX FINDINGS REMAIN UNADDRESSED

Target	Amazon.com, Inc.
Package	com.amazon.mShop.android.shopping
Platform Audited	Android · v32.12.4.100, static analysis of the production APK
Initial Disclosure (R1)	2026-06-20 (REF AMAZONSHOPPING-2026-R1)
Disclosure / Embargo Date	2026-09-19
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	6 (2 Critical, 3 High, 1 Medium)
Correspondence	8 messages sent by RFI-IRFOS across three threads, 2 automated redirect replies, 1 procedural human reply declining payment and requesting a resend of a report already sent, 0 substantive human engagement with any finding
Authorities BCC'd	Luxembourg CNPD - Austrian Datenschutzbehörde (DSB) - CERT.at - Irish Data Protection Commission

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

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

Contents

1	Executive Summary	4
2	Subject & Operator Context	5
3	Engagement Summary	6
4	Findings	7
4.1	C1: Android Health Connect integration reads blood glucose, cervical mucus, and basal body temperature in a shopping app	7
4.2	C2: MyPinPad EMV payment-terminal SDK (1,817 smali classes) undisclosed as an Art. 13(1)(e) payment data recipient	8
4.3	H1: WhisperJoin Alexa IoT-provisioning module (1,449 smali classes) embedded in the shopping application	9
4.4	H2: Alexa voice capture (RECORD_AUDIO, AudioRecordSpeechProvider) wired directly into shopping navigation	9
4.5	H3: ACCESS_BACKGROUND_LOCATION and FOREGROUND_SERVICE_LOCATION enable continuous tracking while the app is backgrounded	10
4.6	M1: DETECT_SCREEN_CAPTURE and DETECT_SCREEN_RECORDING monitor on-device capture attempts without Art. 13 disclosure	10
5	Impact Analysis	11
6	The Complete Chain: From Install to Undisclosed Cross-Domain Data Access	11
7	Data Protection — Article by Article	12
8	Regulatory & Legal Landscape	13
9	Indicators of Compromise	13
10	Disclosure Timeline & Outcome	14
11	What Amazon Shopping Got Right	15
12	Residual Risk & Recommendations	15

Executive Summary

Amazon.com, Inc. operates Amazon Shopping, one of the most widely installed e-commerce applications in the world. The Android application manages account identity, payment methods, delivery addresses, order history, and, through Android Health Connect and an embedded Alexa voice stack, categories of data that have nothing to do with placing an order.

Static analysis of the production application (v32.12.4.100) identified six findings. The app integrates Android Health Connect and reads BloodGlucoseRecord, CervicalMucusRecord, BasalBodyTemperatureRecord, BloodPressureRecord, and HeartRateRecord, GDPR Art. 9(1) special-category health and reproductive data, from any health app a user has separately granted access to, with no proportionate purpose or documented Art. 9(2)(a) consent mechanism specific to a shopping context. A bundled MyPinPad EMV terminal SDK (1,817 smali classes, EMVCo Kernel 3/4/5/6 covering AMEX, Mastercard, JCB, and Discover) gives the application card-present point-of-sale payment-processing capability that is not named as an Art. 13(1)(e) payment data recipient anywhere in Amazon's EU consumer privacy documentation. A WhisperJoin Alexa IoT-provisioning module (1,449 smali classes) and a direct Alexa voice-capture path (RECORD_AUDIO via AudioRecordSpeechProvider) sit inside the shopping navigation flow itself, and ACCESS_BACKGROUND_LOCATION plus FOREGROUND_SERVICE_LOCATION together enable continuous location tracking while the app is backgrounded. A sixth finding, DETECT_SCREEN_CAPTURE and DETECT_SCREEN_RECORDING monitoring for on-device capture attempts, corrects to MEDIUM: a transparency gap rather than a confirmed data-exfiltration path.

RFI-IRFOS disclosed these findings to security@amazon.com on 20 June 2026 under REF AMAZONSHOPPING-2026-R1, BCC to the Luxembourg CNPD (Amazon's lead EU supervisory authority, responsible for a EUR 746 million decision against Amazon in 2021), the Austrian Datenschutzbehörde, and CERT.at. Across the following ten weeks, RFI-IRFOS sent eight messages in total across three related threads. Amazon's security inbox and a secondary cs-reply address each returned one automated redirect message. On 20 July 2026, Amazon's security team did send one genuine human reply, but it was procedural: it declined any paid engagement and asked RFI-IRFOS to resend the full technical report, which had already been sent and confirmed three weeks earlier. Three specific yes/no questions sent on 5 August 2026, regarding the Health Connect consent basis, the MyPinPad disclosure, and the timing of any remediation relative to CNPD contact, were never answered. The stated embargo of 19 September 2026 passed; on that date, Amazon's own correspondence closed and published a companion disclosure covering Amazon Music under REF AMAZONMUSIC-2026-R1, but that publication did not include a single one of Amazon Shopping's six findings, despite both cases having been raised, followed up, and embargoed together in parts of the same correspondence. This report, published 28 days after the Amazon Shopping embargo date, closes that gap.

ID	Severity	Title
C1	CRITICAL	Android Health Connect integration reads blood glucose, cervical mucus, and basal body temperature in a shopping app
C2	CRITICAL	MyPinPad EMV payment-terminal SDK (1,817 smali classes) undisclosed as an Art. 13(1)(e) payment data recipient

ID	Severity	Title
H1	HIGH	WhisperJoin Alexa IoT-provisioning module (1,449 smali classes) embedded in the shopping application
H2	HIGH	Alexa voice capture (RECORD_AUDIO, AudioRecord-SpeechProvider) wired directly into shopping navigation
H3	HIGH	ACCESS_BACKGROUND_LOCATION and FOREGROUND_SERVICE_LOCATION enable continuous tracking while the app is backgrounded
M1	MEDIUM	DETECT_SCREEN_CAPTURE and DETECT_SCREEN_RECORDING monitor on-device capture attempts without Art. 13 disclosure

Subject & Operator Context

Amazon.com, Inc. (Seattle, Washington, USA) operates Amazon Shopping, the company's flagship e-commerce application, available globally through the Google Play Store. The application is one of the most widely installed shopping applications in existence, serving as the primary mobile storefront for Amazon's retail marketplace across most countries where Amazon operates.

The audited application, com.amazon.mShop.android.shopping (v32.12.4.100), handles account identity, stored payment methods, delivery addresses, order history, and product browsing including an AR View feature and an integrated Alexa voice assistant button. It also integrates Android Health Connect and bundles a dedicated EMV payment-terminal SDK and an Alexa device-provisioning module, none of which are functionally necessary to browse or purchase a physical product online.

Amazon is not a new entrant to EU data protection enforcement: the Luxembourg CNPD issued a EUR 746 million administrative fine against Amazon in 2021, at the time the largest GDPR fine on record, for unlawful advertising-related data processing. This disclosure concerns a different application and a different set of findings, but it is addressed to the same corporate entity under the same lead supervisory authority's jurisdiction.

Engagement Summary

RFI-IRFOS sent the initial disclosure (REF AMAZONSHOPPING-2026-R1) to security@amazon.com on 20 June 2026, BCC to the Luxembourg CNPD, the Austrian Datenschutzbehörde, and CERT.at (the CNPD BCC address bounced; the DSB and CERT.at copies were delivered). An automated reply arrived the same day from security@amazon.com, redirecting to Amazon's HackerOne-based Vulnerability Research Program and AWS vulnerability-reporting channels, neither of which applied to a GDPR privacy disclosure already sent to the address the redirect itself designated as correct.

A parallel contact attempt on 25 June 2026 (REF AMAZON-SHOPPING-R2), prompted by an unrelated Amazon Tech Support reply from cs-reply@amazon.de, was escalated by RFI-IRFOS directly to Amazon's EU privacy address and DPO, BCC to Luxembourg's CNPD. RFI-IRFOS followed up again on 27 June 2026, stating explicitly that the automated security-channel redirect was not a substantive reply, restating the Health Connect and MyPinPad findings in full, and setting a 29 June 18:00 CET deadline for a human response.

On 20 July 2026, Amazon's security team (vrp-researchers@amazon.com) sent the one human reply received in this entire correspondence, addressing both Amazon Shopping and a parallel Amazon Music disclosure together. The reply declined any paid engagement and asked RFI-IRFOS to send the full technical report in writing, with all technical detail for each finding, a report that had in fact already been sent in full three weeks earlier. RFI-IRFOS replied on 21 July 2026 clarifying this, and followed up again on 15 August 2026 noting 25 days had passed since that clarification without any further reply.

A direct follow-up to security@amazon.com on 5 August 2026 restated the Health Connect and MyPinPad findings at the 46-day mark and posed three specific yes/no questions: whether a documented Art. 9(2)(a) consent mechanism exists for each Health Connect data type accessed, whether MyPinPad is named as an Art. 13(1)(e) payment processor, and whether Health Connect access would be scoped to a proportionate purpose before or after CNPD contact. None of the three questions were ever answered. Further follow-ups on 29 August and 4 September 2026, addressed to vrp-researchers@amazon.com and restating both the Amazon Shopping and Amazon Music findings together, also went unanswered. On 19 September 2026, the stated embargo date, Amazon's own correspondence record shows a publication notice was sent closing and publishing the companion Amazon Music case under REF AMAZONMUSIC-2026-R1 — but that notice's six published findings are all Amazon Music findings; none of Amazon Shopping's six findings appear in it. No further contact regarding Amazon Shopping specifically has been received since 4 September 2026.

Findings

C1: Android Health Connect integration reads blood glucose, cervical mucus, and basal body temperature in a shopping app

CRITICAL (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 7.9) — Art. 9 special category health and reproductive data accessible to an e-commerce app

```
BloodGlucoseRecord.kt      BloodPressureRecord.kt
BasalBodyTemperatureRecord.kt  CervicalMucusRecord.kt  <- reproductive/fertility
HeartRateRecord.kt          SleepSessionRecord.kt
NutritionRecord.kt          BodyFatRecord.kt
BodyTemperatureRecord.kt     ExerciseSessionRecord.kt
HydrationRecord.kt          WeightRecord.kt / StepsRecord.kt

HealthConnectClientImpl.kt, ServiceBackedHealthDataClient,
RegisterForDataNotificationsRequest$Builder

Connected endpoints (APK strings): health.amazon.com,
health.amazon.com/(prime|onemedical|a|ap), pharmacy.amazon.com,
clinic.amazon.com, PharmacyModalConfig$Mapper, CLINIC_URL_PATTERN
```

Impact: RFI-IRFOS blast-radius escalation: raised from HIGH/7.9 to CRITICAL. Class names extracted directly from the production APK confirm BloodGlucoseRecord, BloodPressureRecord, BasalBodyTemperatureRecord, CervicalMucusRecord, HeartRateRecord, SleepSessionRecord, NutritionRecord, BodyFatRecord, BodyTemperatureRecord, ExerciseSessionRecord, HydrationRecord, WeightRecord, and StepsRecord as Health Connect record types the application is built to read, alongside connected endpoints health.amazon.com, pharmacy.amazon.com, and clinic.amazon.com. Blood glucose, basal body temperature, cervical mucus, and blood pressure are special-category data under Art. 9(1), requiring an explicit Art. 9(2)(a) consent basis distinct from general app permissions. A user who installs Amazon Shopping to buy a physical product, and who has separately granted a health app access to Android Health Connect, did not consent at install time to their reproductive-health or diabetes-indicator data becoming accessible to an e-commerce application. The population affected is not a narrow subset: it is every Health Connect user who also installs one of the world's most widely distributed shopping apps.

C2: MyPinPad EMV payment-terminal SDK (1,817 smali classes) undisclosed as an Art. 13(1)(e) payment data recipient

CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7) — undisclosed card-present EMV terminal capability bundled into a consumer shopping app

```
com/mypinpad/softpos/emv/terminal/config/Kernel3ConfigDto <- AMEX
com/mypinpad/softpos/emv/terminal/config/Kernel4ConfigDto <- Mastercard
com/mypinpad/softpos/emv/terminal/config/Kernel5ConfigDto <- JCB
com/mypinpad/softpos/emv/terminal/config/Kernel6ConfigDto <- Discover
com/mypinpad/softpos/emv/terminal/config/TlvConfigData
com/mypinpad/tsdk/api/TerminalSdk
GetCardDataResultCallbackKt, TransactionNotAuthorised, CardScheme
```

1,817 smali classes total

Impact: RFI-IRFOS blast-radius escalation: raised from HIGH/8.7 to CRITICAL because MyPinPad's undisclosed EMV terminal capability sits inside one of the world's most widely installed shopping apps, giving an ordinary transparency gap a blast radius far larger than a typical undisclosed-SDK finding. `com/mypinpad/softpos/emv/terminal/config/Kernel3ConfigDto` through `Kernel6ConfigDto` implement the EMVCo-standard processing kernels for AMEX, Mastercard, JCB, and Discover respectively; `TlvConfigData` handles the raw Tag-Length-Value format in which physical payment cards transmit account numbers and cryptographic tokens during contactless transactions. Combined with the application's NFC permission, Amazon Shopping carries the technical capability of a point-of-sale payment terminal. MyPinPad Ltd is not identified as a named Art. 28 payment data processor anywhere in Amazon's EU consumer privacy documentation reviewed for this audit, a direct Art. 13(1)(e) transparency failure for a data recipient capable of handling raw card data.

H1: WhisperJoin Alexa IoT-provisioning module (1,449 smali classes) embedded in the shopping application

HIGH (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 7.1) — undisclosed IoT device-provisioning capability exceeding shopping functionality

WhisperJoin Alexa IoT device-provisioning module
1,449 smali classes, embedded in com.amazon.mShop.android.shopping

Impact: WhisperJoin is Amazon's Alexa smart-home device-provisioning protocol, present as a 1,449-class module inside the shopping application's binary. WhisperJoin handles Wi-Fi credential exchange and device pairing for Alexa-compatible IoT hardware, a function entirely unrelated to browsing or purchasing products. Its presence is not disclosed as a distinct data-processing activity in Amazon's EU consumer privacy documentation reviewed for this audit, and it is not clear from static analysis alone what scope of network-configuration or device-identifier data this module can access or transmit from within a shopping-app context, an open question this report cannot resolve without a documented answer from Amazon.

H2: Alexa voice capture (RECORD_AUDIO, AudioRecordSpeechProvider) wired directly into shopping navigation

HIGH (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, 7.0) — microphone capture path embedded in the shopping flow itself

android.permission.RECORD_AUDIO
AudioRecordSpeechProvider -- Alexa voice-capture provider class,
present in the shopping navigation module

Impact: The application declares android.permission.RECORD_AUDIO and bundles AudioRecordSpeechProvider, an Alexa voice-capture class, directly within the shopping navigation stack rather than as an isolated, clearly-gated voice-search feature. The Alexa voice button is visible UI, not hidden, which this report credits in the section below, but visibility of a button is not the same as a documented Art. 6(1)(a) consent basis distinguishing deliberate voice-search activation from any other microphone-activation path the bundled Alexa stack may expose. No Art. 9 health-data capture via voice was identified during this audit; the finding is the absence of a documented, isolated consent gate for microphone access inside a shopping context, not a confirmed instance of unauthorized recording.

H3: ACCESS_BACKGROUND_LOCATION and FOREGROUND_SERVICE_LOCATION enable continuous tracking while the app is backgrounded

HIGH (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 7.0)
— continuous location collection independent of active app use

```
android.permission.ACCESS_BACKGROUND_LOCATION
android:foregroundServiceType="location" (declared service)
```

Impact: android.permission.ACCESS_BACKGROUND_LOCATION together with a declared FOREGROUND_SERVICE_LOCATION service type gives the application the technical capability to collect location data continuously while the app is backgrounded or the screen is off, not only while a user is actively browsing or tracking a delivery. Delivery-estimate and store-locator functionality are plausible justifications for foreground location access; neither requires standing background collection. No distinct consent gate separating background from in-use location collection was identified in the application's consent flow during this audit, a data-minimisation gap under Art. 5(1)(c) independent of whether background collection is currently being exercised in practice.

M1: DETECT_SCREEN_CAPTURE and DETECT_SCREEN_RECORDING monitor on-device capture attempts without Art. 13 disclosure

MEDIUM (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.9) — undisclosed monitoring capability, corrected from the original HIGH working label

```
android.permission.DETECT_SCREEN_CAPTURE
android.permission.DETECT_SCREEN_RECORDING
```

Impact: Corrected from the original audit's working HIGH label to MEDIUM: DETECT_SCREEN_CAPTURE and DETECT_SCREEN_RECORDING detect, but do not themselves exfiltrate, a user's own on-device screenshot or screen-recording attempts. This is architecturally identical to a legitimate anti-fraud measure seen elsewhere in this audit series, and this report does not allege a confirmed data flow comparable in severity to C1 or C2. The finding that remains is narrower: the capability is not named or explained in Amazon's EU consumer privacy documentation reviewed for this audit, leaving open whether it is used solely for fraud prevention or also to detect when a user attempts to document pricing, dark patterns, or other on-screen content for their own records, a distinction Amazon has not made in writing.

Impact Analysis

C1 and C2 together describe an e-commerce application that reaches well beyond commerce in the categories of data it is built to access. C1 means a Health Connect user who installs Amazon Shopping for an entirely unrelated purpose has reproductive-health and diabetes-marker data structurally accessible to that shopping app, with no shopping-specific purpose ever articulated for that access. C2 means the same application carries a card-present payment-terminal capability that is not named to EU consumers as a payment data recipient at all.

H1 through H3 describe a pattern rather than three isolated gaps: an Alexa IoT-provisioning module (H1) and a direct Alexa microphone-capture path (H2) both sit inside the shopping flow itself, functions with no shopping-specific purpose, while background location collection (H3) extends tracking beyond the window in which a user is actually engaging with the app. M1's screen-capture detection is the weakest finding here and is scored accordingly, but it shares the same root issue as the findings above it: capabilities present in the binary that are never named or explained to the EU consumers whose devices run them.

The Complete Chain: From Install to Undisclosed Cross-Domain Data Access

Step 1 — Install: Download Amazon Shopping (com.amazon.mShop.android.shopping) from the Google Play Store. No special permissions are required at install time beyond the application's own declared manifest.

Step 2 — Extract: Pull the production APK (v32.12.4.100) from an enrolled test device via adb, or obtain it directly from Play.

Step 3 — Decompile: Run apktool against the base APK. Health Connect record-type classes, the MyPinPad EMV terminal package tree, the WhisperJoin module, and the Alexa voice-capture provider are all present in plaintext class and string form.

Step 4 — Health data exposure: For any user who has separately granted a health app access to Android Health Connect, the shopping app's bundled Health Connect client (C1) is structurally capable of reading blood glucose, cervical mucus, basal body temperature, and heart rate records the moment Health Connect permission is granted to the shopping app for any other declared purpose.

Step 5 — Payment surface: The bundled MyPinPad EMV terminal SDK (C2) gives the application card-present, contactless EMV-processing capability for four major card schemes, a capability never named to the EU consumer as a distinct payment data recipient.

Step 6 — Ancillary capability load: While browsing or shopping, the WhisperJoin IoT-provisioning module (H1) and the Alexa voice-capture path (H2) sit active in the same navigation flow, neither isolated behind a shopping-specific justification. ACCESS_BACKGROUND_LOCATION (H3) extends the application's location awareness beyond the window of active use. DETECT_SCREEN_CAPTURE and DETECT_SCREEN_RECORDING (M1) give the application visibility into the user's own attempts to document what is on screen.

By the time a single browsing session is complete, a user's Health Connect data, payment-terminal-capable processing surface, IoT-provisioning module, microphone-capture path, and background location are all structurally present and reachable inside what presents itself to the user as a shopping app, none of it requiring any attacker capability to observe: it is the application's shipped, designed behaviour, visible to anyone who decompiles the public

binary.

Data Protection — Article by Article

Art. 9(1)/Art. 9(2)(a) GDPR — Special categories of data: C1's Health Connect integration structurally reads blood glucose, cervical mucus, basal body temperature, and blood pressure records, all Art. 9(1) special-category data. Art. 9(1) prohibits this processing absent an explicit Art. 9(2)(a) consent basis documented specifically for a shopping context, which this audit did not find.

Art. 13(1)(e) GDPR — Transparency, recipients of data: C2's MyPinPad EMV terminal integration and H1's WhisperJoin IoT-provisioning module were not identified as disclosed data recipients or distinct processing activities in the EU consumer privacy documentation reviewed for this audit.

Art. 28 GDPR — Processor: MyPinPad Ltd was not identified as a disclosed Art. 28 processor for payment data (C2).

Art. 5(1)(b) GDPR — Purpose limitation: C1's health-data access and H2's Alexa voice-capture path, both embedded in a shopping application, exceed the stated operational purpose of browsing and purchasing products.

Art. 5(1)(c) GDPR — Data minimisation: H3's background-location capability and H1's IoT-provisioning module both exceed what order browsing, purchase, or delivery-estimate functionality requires.

Art. 6(1)(a) GDPR — Consent: H2's microphone-capture path and H3's background-location collection both lack a documented, isolated consent gate distinct from general app permissions.

Art. 13(1)(c) GDPR — Transparency, purpose of processing: M1's capture-detection capability is present without a stated purpose distinguishing fraud prevention from monitoring of a user's own documentation attempts.

Art. 33(4) GDPR — Notification of a personal data breach: RFI-IRFOS's 5 August 2026 follow-up placed on record that, if Amazon treats any of C1-C2 as a personal data breach, the 72-hour notification clock runs from the date Amazon became aware, at the latest 20 June 2026, the date of initial disclosure.

Regulatory & Legal Landscape

RFI-IRFOS BCC'd the Luxembourg CNPD throughout this correspondence as Amazon's lead EU supervisory authority of record, the same authority that issued a EUR 746 million administrative decision against Amazon in 2021. The Austrian Datenschutzbehörde and CERT.at were BCC'd as the inferred relevant regulators under Art. 3(2) extraterritorial scope for a globally distributed Play Store application processing data of Austrian and EU-resident users; the Irish Data Protection Commission was added to BCC from 27 June 2026 onward given Amazon's EU corporate presence routes substantially through Ireland.

Amazon.com, Inc. is additionally subject to the US FTC Act Section 5 unfair-or-deceptive-practices framework for undisclosed data-collection practices generally, and to state-level US privacy statutes (including the California Consumer Privacy Act/CPRA) for the same conduct toward US residents.

Fine exposure under GDPR, to the extent EU-resident users are processed under Art. 3(2): Art. 83(5) applies to Art. 9 special-category violations (C1) — administrative fines up to EUR 20,000,000 or 4% of total worldwide annual turnover, whichever is higher, a percentage basis that, applied to Amazon's global turnover, dwarfs the 2021 CNPD decision in absolute terms. Art. 83(4) applies to the Art. 5, 6, 13, and 28 violations (C2, H1-H3, M1) — up to EUR 10,000,000 or 2% of total worldwide annual turnover.

Indicators of Compromise

The following identifiers and class names were extracted from the production APK (v32.12.4.100, audited 2026-06-20) via static analysis only. No Amazon servers, accounts, or infrastructure were probed.

```
C1 -- Health Connect record classes
    BloodGlucoseRecord, BloodPressureRecord, BasalBodyTemperatureRecord,
    CervicalMucusRecord, HeartRateRecord, SleepSessionRecord
    Connected endpoints: health.amazon.com, pharmacy.amazon.com,
    clinic.amazon.com

C2 -- MyPinPad EMV terminal packages
    com/mypinpad/softpos/emv/terminal/config/Kernel3-6ConfigDto
    com/mypinpad/tsdk/api/TerminalSdk (1,817 smali classes)

H1 -- WhisperJoin IoT-provisioning module (1,449 smali classes)

H2 -- Alexa voice-capture provider
    AudioRecordSpeechProvider, android.permission.RECORD_AUDIO

H3 -- Background location permissions
    android.permission.ACCESS_BACKGROUND_LOCATION

M1 -- Capture-detection permissions
    android.permission.DETECT_SCREEN_CAPTURE
    android.permission.DETECT_SCREEN_RECORDING
```

Disclosure Timeline & Outcome

2026-06-20 Initial disclosure (R1, REF AMAZONSHOPPING-2026-R1) sent to security@amazon.com. BCC: Luxembourg CNPD (bounced), Austrian DSB, CERT.at. Automated redirect reply received the same day from security@amazon.com, pointing to Amazon's HackerOne VRP and AWS vulnerability-reporting channels.

2026-06-25 A separate automated reply from cs-reply@amazon.de on an unrelated general inquiry thread is escalated by RFI-IRFOS (REF AMAZON-SHOPPING-R2) directly to Amazon's EU privacy address and DPO, BCC Luxembourg CNPD.

2026-06-27 7-day follow-up to security@amazon.com, CC press@amazon.com, BCC DSB/CERT.at/Irish DPC, stating explicitly that the automated redirect does not constitute a substantive reply and restating both CRITICAL findings in full. Deadline set for 29 June 2026 18:00 CET; none met.

2026-07-20 Amazon's security team (vrp-researchers@amazon.com) sends the only human reply received in this correspondence, addressing Amazon Shopping and Amazon Music jointly: declines any paid engagement and requests the full technical report be resent, though it had already been sent and confirmed three weeks earlier.

2026-07-21 RFI-IRFOS replies clarifying that the requested report was already sent.

2026-08-05 46-day follow-up to security@amazon.com restating the Health Connect and MyPinPad findings and posing three specific yes/no questions on the Art. 9(2)(a) consent basis, the MyPinPad Art. 13(1)(e) disclosure, and remediation timing relative to CNPD contact. None of the three questions were ever answered.

2026-08-15 Follow-up to vrp-researchers@amazon.com noting 25 days since the 21 July clarification without further reply.

2026-08-29 Follow-up to vrp-researchers@amazon.com, restating both Amazon Shopping's and Amazon Music's findings together, 14 days since the prior message.

2026-09-04 Follow-up to vrp-researchers@amazon.com, 6 days since the prior message, 15 days before the stated embargo.

2026-09-19 Stated embargo date reached. Amazon's correspondence record shows a publication notice sent the same day closing and publishing the companion Amazon Music case under REF AMAZONMUSIC-2026-R1. That notice's published findings are exclusively Amazon Music findings; none of Amazon Shopping's six findings are included in it, and no separate publication notice or closure for Amazon Shopping was sent at that time.

2026-10-17 This report published, 28 days after the Amazon Shopping embargo date. All six findings confirmed unaddressed on the basis of the correspondence record; no re-verification download was performed for this report.

What Amazon Shopping Got Right

targetSdk 36 is current, and minSdk 28 (Android 9) is a defensible modern security baseline for an application with this install base. No plaintext Firebase API keys were found in the APK's assets during this audit, a credential-hygiene standard several other applications in this disclosure series did not meet. The AR View shopping feature is disclosed and genuinely useful, not a hidden tracking surface. The Alexa voice button in the shopping interface is visible UI, not a concealed activation path.

These choices do not offset the findings in this report. A visible button inviting a user to use voice search does not, by itself, establish a documented consent basis for the microphone-capture path and IoT-provisioning module bundled behind it (H1, H2), and a clean credential posture on Firebase keys says nothing about whether Health Connect data or MyPinPad's payment-processing capability are properly disclosed and consented to (C1, C2). Security hygiene in credential handling and UI transparency in one feature do not substitute for data-minimisation and purpose-limitation discipline in the application's broader data model.

Residual Risk & Recommendations

C1 — Immediate: Document a formal necessity and proportionality assessment for Health Connect access specific to the shopping-app context, scoped to the actual feature (if any) that requires it. Implement a distinct Art. 9(2)(a) consent gate for each special-category Health Connect record type the app can read, separate from general app permissions. Where no shopping-specific feature requires a given record type, remove read access to it.

C2 — Immediate: Disclose MyPinPad Ltd as a named Art. 28 payment data processor in Amazon's EU consumer privacy notice. Document the specific shopping-app feature, if any, that requires card-present EMV terminal capability, and restrict the SDK's active scope to that feature alone if retained.

H1 — Transparency: Disclose the WhisperJoin IoT-provisioning module as a distinct processing activity, or remove it from the shopping application if device-provisioning functionality is not an intended shopping-app feature.

H2 — Governance: Implement a consent gate for microphone activation that is specific to deliberate voice-search initiation, distinct from any other activation path the bundled Alexa stack may expose, and document the Art. 6(1)(a) basis for each.

H3 — Structural: Scope ACCESS_BACKGROUND_LOCATION to a specific, disclosed, time-bounded feature (e.g., active delivery tracking) rather than standing background access, and implement a distinct consent gate separating background from in-use location collection.

M1 — Transparency: State in the Art. 13 privacy notice whether DETECT_SCREEN_CAPTURE and DETECT_SCREEN_RECORDING are used solely for fraud/anti-scraping purposes, and confirm the capability is not used to detect or discourage a user's own documentation of on-screen pricing or interface behaviour.

Across all findings: establish a single, monitored intake address for GDPR disclosures that does not auto-redirect to a bug-bounty program scoped to security vulnerabilities rather than privacy-architecture findings, and ensure a human response addresses the substance of a disclosure rather than requesting a resend of material already received and confirmed.

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethnergasse 25/10, 8020 Graz, Austria All findings derive from static root-level analysis of the published application using publicly available tooling. No Amazon servers, accounts, or infrastructure were probed. Technical evidence is archived under chain of custody and will be provided to regulatory authorities on request. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF AMAZONSHOPPING-2026.