



Security & Privacy Disclosure, Final Report

[AutoScout24 \(com.autoscout24\)](https://com.autoscout24)

Cleartext HTTP explicitly configured for the financing pre-enquiry endpoint and the Mediarithmics customer-data platform, a hardcoded Firebase production API key and database URL, three pre-consent SDK auto-initializations, four BOOT_COMPLETED receivers paired with IMEI access on a vehicle-financing platform, and three undisclosed behavioral-data processors, unresolved through 109 days and a 19-day-overdue embargo, with two genuine replies – a bug-bounty-program deflection and a legal-counsel acknowledgment that corrected a dead privacy mailbox but never answered any of four GDPR questions

**PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 28
SEPTEMBER 2026, FIVE FINDINGS REMAIN UNADDRESSED**

Target	AutoScout24 Engine GmbH / AutoScout24 GmbH, Munich, Germany (Hellman & Friedman private equity, ~28 million monthly users, ~EUR 2.5 billion+ valuation)
Package	com.autoscout24
Platform	Android, static analysis (176.6 MB APK, 96,534 smali classes)
Initial Disclosure (R1)	2026-06-30 (REF COM.AUTOScout24)
Disclosure / Embargo Date	2026-09-28
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	5 (2 Critical, 3 High)
Correspondence	10 messages sent by RFI-IRFOS over 96 days (30 June through 3 September 2026) to security@autoscout24.com, CC press@autoscout24.com, the Austrian DSB, CERT.at, and the Bavarian data protection authority (BayLDA). datenschutz@autoscout24.com, the address AutoScout24 publishes as its data protection contact, hard-bounced on every attempt (30 June, 6 July, 24 July) and was dropped after. Two genuine replies were received: a 17 August 2026 bug-bounty-program deflection from security@autoscout24.com, and a 20 August 2026 message from Senior Legal Counsel Darko Radonjic acknowledging the matter was under review and correcting the contact address to as24-datenschutz@autoscout24.com. Neither reply answered any of the four GDPR questions put to AutoScout24. A follow-up deadline of 15 September 2026 and the 28 September 2026 embargo both passed without further word; the only response after 3 September 2026 was an automated customer-service acknowledgment, not a substantive reply.
Authorities CC'd	Österreichische Datenschutzbehörde (DSB), Austria; CERT.at; Bayerisches Landesamt für Datenschutzaufsicht (BayLDA), Germany

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

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

Contents

1	Executive Summary	4
2	Subject & Operator Context	5
3	Engagement Summary	6
4	Findings	6
4.1	C1: Cleartext HTTP explicitly permitted for the financing API and the Mediarithmics customer-data platform	7
4.2	C2: Firebase API key and production database URL hardcoded, repeated four times in the same file	8
4.3	H1: Firebase, Google Mobile Ads, and Adjust all auto-initialize via Content-Provider before any consent screen	9
4.4	H2: Four BOOT_COMPLETED receivers and READ_PHONE_STATE (IMEI access) on a vehicle-financing platform	10
4.5	H3: Adobe Experience Platform, Iterable, and Mediarithmics process behavioral data without being identifiably named as processors	11
5	Impact Analysis	11
6	The Complete Chain: Ten Messages Across 96 Days, Two Replies and Zero Answers	12
7	Disclosure Timeline & Outcome	13
8	Data Protection — Article by Article	14
9	Regulatory Landscape & Fine Exposure	15
10	Indicators of Compromise	15
11	Residual Risk & Recommendations	16

Executive Summary

AutoScout24 Engine GmbH / AutoScout24 GmbH (Munich, Germany), Europe's largest car marketplace with roughly 28 million monthly users and a valuation exceeding EUR 2.5 billion, publishes com.autoscout24 on Google Play. A static analysis identified five findings, two CRITICAL and three HIGH, spanning an explicitly configured cleartext-transport exception on the platform's own financing endpoint, a hardcoded production credential, three pre-consent SDK initializations, a permanent-device-identifier permission paired with boot-time receivers on a credit-intent platform, and undisclosed behavioral-data processors.

The app's network security configuration explicitly sets `cleartextTrafficPermitted="true"` for `rest.autoscout24.com` – the endpoint that carries financing pre-enquiries, vehicle valuations, and user profile data – for all EU marketplace domains (`ww2.autoscout24.de/it/es/fr/nl`), and for `api.mediarithmics.com`, a real-time-bidding customer data platform. This is not a default left in place; it is an entry someone wrote, enabling unencrypted transport of financing-intent data on a platform where users submit income and creditworthiness information (C1). A Firebase API key and the app's production database URL are hardcoded in `res/values/strings.xml`, with the key repeated four times under different string names in the same file (C2). Firebase, Google Mobile Ads, and Adjust all auto-initialize via `ContentProvider` at `initOrder="100"`, before any consent screen can render (H1). Four `RECEIVE_BOOT_COMPLETED` receivers start tracking processes at device boot, and `READ_PHONE_STATE` grants access to the IMEI – a permanent, non-rotating device identifier – on a platform that records vehicle purchase intent, price, and financing readiness, with no stated purpose in the privacy policy (H2). Adobe Experience Platform, Iterable, and the Mediarithmics CDP all process user behavioral and purchase-intent data without being identifiably named as processors in AutoScout24's privacy disclosures (H3).

RFI-IRFOS disclosed these findings on 30 June 2026 to `security@autoscout24.com` and `datenschutz@autoscout24.com`, CC `press@autoscout24.com`, the Austrian DSB, CERT.at, and the BayLDA, fixing a 90-day embargo of 28 September 2026. `datenschutz@autoscout24.com` hard-bounced immediately and on every subsequent attempt (6 July, 24 July 2026); `security@autoscout24.com` was the only address that ever accepted mail. Follow-ups went out on 6 July, 17 July, 23 July, 31 July, and twice on 9 August 2026, restating the three original questions – the Art. 32(1)(a) basis for the cleartext configuration, the Art. 6(1) basis for IMEI access plus any Art. 33 notification to the BayLDA, and the Art. 28 processing agreement for Mediarithmics – without any reply for 49 days. On 17 August 2026, `security@autoscout24.com` broke the silence with a reply directing RFI-IRFOS to AutoScout24's Intigriti-hosted vulnerability disclosure program. RFI-IRFOS declined this redirection on 18 August 2026 (sent twice, 23 minutes apart), explaining why a bug-bounty intake queue cannot discharge GDPR accountability obligations owed to a controller, restating the findings, and adding a fourth question – whether AutoScout24's data protection team is even aware of this disclosure, given the dead mailbox – with a deadline of 25 August 2026.

On 20 August 2026, Darko Radonjic, AutoScout24's Senior Legal Counsel, replied in German: AutoScout24 was reviewing the matter described and might come back to RFI-IRFOS at a later point, and the mailbox RFI-IRFOS had been using, `datenschutz@autoscout24.com`, was never AutoScout24's actual privacy contact – the correct address, per AutoScout24's own privacy notice (item 9), is `as24-datenschutz@autoscout24.com`. This is a genuine, substantive-sounding reply from a named legal professional, and it corrected a real defect in AutoScout24's published contact information; it did not, however, answer any of the four GDPR questions, and no further word followed. RFI-IRFOS wrote again on 3 September 2026 to `security@autoscout24.com`, `darko.radonjic@autoscout24.com`, `press@autoscout24.com`, and the newly-corrected `as24-datenschutz@autoscout24.com`, noting the 25 August dead-

line had passed unanswered and setting a final deadline of 15 September 2026. The only reply this message drew was an automated AutoScout24 customer-service acknowledgment 36 seconds later – a generic auto-responder, not a review or a legal reply. 15 September 2026 passed with nothing further, and so did the 28 September 2026 embargo. This report publishes 19 days after embargo, 109 days after the original disclosure, with all five findings unaddressed and none of the four questions ever answered.

ID	Severity	Title
C1	CRITICAL	Cleartext HTTP explicitly permitted for the financing API and the Mediarithmics customer-data platform
C2	CRITICAL	Firebase API key and production database URL hard-coded, repeated four times in the same file
H1	HIGH	Firebase, Google Mobile Ads, and Adjust all auto-initialize via ContentProvider before any consent screen
H2	HIGH	Four BOOT_COMPLETED receivers and READ_PHONE_STATE (IMEI access) on a vehicle-financing platform
H3	HIGH	Adobe Experience Platform, Iterable, and Mediarithmics process behavioral data without being identifiably named as processors

Subject & Operator Context

AutoScout24 is Europe's largest car marketplace, operated by AutoScout24 Engine GmbH and AutoScout24 GmbH (Munich, Germany, Hellman & Friedman private equity backing), with roughly 28 million monthly users and a valuation exceeding EUR 2.5 billion. The Android app processes financing pre-enquiries, vehicle valuations, and purchase-intent data for this user base directly. A platform of this scale explicitly configuring cleartext transport on its own financing endpoint, and running a dead data protection mailbox for the duration of a disclosure, raises the stakes of each finding below beyond what the same findings would mean for a smaller operator.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 30 June 2026 to security@autoscout24.com and datenschutz@autoscout24.com, CC press@autoscout24.com, the Austrian DSB, CERT.at, and the BayLDA, fixing a 90-day embargo of 28 September 2026. datenschutz@autoscout24.com hard-bounced on 30 June, 6 July, and 24 July 2026 and was dropped after the third failure; security@autoscout24.com remained the only address that ever accepted mail.

Five follow-ups (6 July, 17 July, 23 July, 31 July, and twice on 9 August 2026) restated the original three questions without drawing a reply for 49 days. On 17 August 2026, security@autoscout24.com replied for the first time, redirecting RFI-IRFOS to AutoScout24's Intigriti vulnerability disclosure program. RFI-IRFOS declined this redirection in detail on 18 August 2026, restating the findings and adding a fourth question, with a deadline of 25 August 2026.

On 20 August 2026, Senior Legal Counsel Darko Radonjic replied in German, stating the matter was under review and might be followed up on later, and correcting the published data protection address to as24-datenschutz@autoscout24.com. This was a genuine, named-individual reply that fixed a real contact-channel defect, but it answered none of the four questions. RFI-IRFOS followed up a final time on 3 September 2026 to the expanded recipient list including the corrected address, setting a final deadline of 15 September 2026; the only response was an automated customer-service acknowledgment 36 seconds later. Neither the 15 September deadline nor the 28 September embargo drew any further word. This report publishes 19 days after embargo, with no answer ever given to any of the four questions across 10 messages and 96 days of active correspondence.

Findings

C1: Cleartext HTTP explicitly permitted for the financing API and the Mediarithmics customer-data platform

CRITICAL (CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 8.3) — a network-adjacent attacker can intercept financing pre-enquiries and behavioral-targeting data in plaintext, by configuration rather than default

```
<domain-config cleartextTrafficPermitted="true">
  <domain includeSubdomains="true">ww2.autoscout24.de</domain>
  <domain includeSubdomains="true">ww2.autoscout24.it</domain>
  <domain includeSubdomains="true">ww2.autoscout24.es</domain>
  <domain includeSubdomains="true">ww2.autoscout24.fr</domain>
  <domain includeSubdomains="true">ww2.autoscout24.nl</domain>
  <domain includeSubdomains="true">rest.autoscout24.com</domain>
  <domain includeSubdomains="true">s3-us-west-2.amazonaws.com</domain>
  <domain includeSubdomains="true">api.mediarithmics.com</domain>
</domain-config>
```

rest.autoscout24.com carries financing pre-enquiries and vehicle valuation requests.
api.mediarithmics.com is a real-time-bidding customer data platform receiving behavioral data.

Art. 32(1)(a) basis for this configuration, and any Art. 35 DPIA covering the combination of

financing-intent data with unencrypted transport: never answered across four written questions.

Impact: res/xml/network_security_config.xml explicitly sets cleartextTrafficPermitted="true" for rest.autoscout24.com – the endpoint carrying financing pre-enquiries, vehicle valuations, and user profile data – for all EU marketplace domains (ww2.autoscout24.de/it/es/fr/nl), and for api.mediarithmics.com, a real-time-bidding customer data platform. Android honors this configuration: any HTTP connection the app opens to these domains is permitted to travel unencrypted. A party positioned on the network path – an open Wi-Fi network, a compromised router, a malicious proxy – can read or alter financing-intent data, including income and creditworthiness signals users submit when requesting pre-approval, in plaintext. This is not a default Android leaves in place; cleartextTrafficPermitted must be explicitly declared, meaning someone at AutoScout24 wrote this entry for a financing endpoint on a platform of this scale.

C2: Firebase API key and production database URL hardcoded, repeated four times in the same file

CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 8.1) — a functioning Firebase API key and the app's production database URL hardcoded verbatim, extractable from any installed copy of Europe's largest car marketplace app

```
google_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to
AutoScout24 in R1]
firebase_database_url: [REDACTED IN PUBLIC REPORT -- disclosed privately to
AutoScout24 in R1]
```

The key is repeated under four separate string names in the same file:
google_api_key, google_crash_reporting_api_key, m, google_app_id

Observed fact vs. inference: the presence of these values in the binary is an observed fact.
Whether Firebase Security Rules independently restrict database access regardless of key exposure is the operator's determination under Art. 5(2) accountability, not verifiable from the client binary alone, and was never addressed in any reply.

Impact: res/values/strings.xml hardcodes a functioning-format Google API key and the app's Firebase production database URL, present verbatim in every distributed copy of com.autoscout24. The key appears four times in the same file, under google_api_key, google_crash_reporting_api_key, m, and google_app_id. Any party extracting the APK obtains both values directly, enabling quota-exhaustion attacks against AutoScout24's Google Cloud billing and, if the underlying Firebase Security Rules are misconfigured, direct access to the production database at autoscout24-android.firebaseio.com. Firebase keys being a documented, expected part of client binaries does not by itself satisfy Art. 32(1)(b); it shifts the question to whether the Security Rules and quota controls behind the key are independently adequate, which cannot be verified from the client binary alone and was never confirmed in correspondence.

H1: Firebase, Google Mobile Ads, and Adjust all auto-initialize via ContentProvider before any consent screen

HIGH (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.6)
— three separate SDKs initialize at app start via the ContentProvider mechanism, before a consent screen can render, on a platform with a car-financing use case

```
<provider android:name="com.google.firebase.provider.FirebaseInitProvider"
  android:authorities="com.autoscout24.firebaseinitprovider"
  android:initOrder="100" android:directBootAware="true"/>
<provider android:name="com.google.android.gms.ads.MobileAdsInitProvider"
  android:authorities="com.autoscout24.mobileadsinitprovider"
  android:initOrder="100"/>
<provider android:name="com.adjust.sdk.SystemLifecycleContentProvider"
  android:authorities="com.autoscout24.adjust-lifecycle-provider"/>
```

All three initialize via the ContentProvider mechanism at app start, before
Application.onCreate()
and before any consent screen can render.

Impact: FirebaseInitProvider, MobileAdsInitProvider, and Adjust's SystemLifecycleContentProvider are all declared in the manifest with android:initOrder="100", meaning Android instantiates them before Application.onCreate() and therefore before any consent screen the app might show. Firebase Performance, Google Mobile Ads, and Adjust attribution tracking all begin before a user has any opportunity to decline. Art. 7 GDPR requires that consent precede processing, not follow it; a ContentProvider-based auto-init structurally inverts that sequence regardless of what the consent screen later presents.

H2: Four BOOT_COMPLETED receivers and READ_PHONE_STATE (IMEI access) on a vehicle-financing platform

HIGH (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.8)
— permanent, non-rotating device fingerprinting via IMEI, combined with four boot-time receivers, on a platform that records purchase intent, vehicle price, and financing readiness

4x android.intent.action.BOOT_COMPLETED – receivers start at device boot, before app launch

android.permission.READ_PHONE_STATE – grants IMEI access (permanent, non-rotating identifier)

Stated purpose for READ_PHONE_STATE in AutoScout24's privacy policy: not identified.

Art. 6(1) legal basis for IMEI processing on a financing-intent platform: asked in writing on

2026-06-30, 2026-07-17, 2026-08-09, and 2026-09-03; never answered.

Art. 33 notification to the BayLDA for this configuration: asked in writing on the same four

occasions; never confirmed or denied.

Impact: Four separate android.intent.action.BOOT_COMPLETED receivers start tracking processes at device startup, before the app is opened or any consent is given. READ_PHONE_STATE grants access to the IMEI, a permanent, non-rotating device identifier usable for persistent device fingerprinting independent of app reinstalls or ad-ID resets. On a platform recording vehicle purchase intent, price, and financing readiness, IMEI-based fingerprinting links a durable credit-intent profile to a device identifier that cannot be changed by the user. No purpose for this permission is stated in AutoScout24's privacy policy, and the Art. 6(1) legal basis for it was asked directly across three separate messages and never answered.

H3: Adobe Experience Platform, Iterable, and Mediarithmics process behavioral data without being identifiably named as processors

HIGH (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.0)
 — three separate behavioral-data processors operate on purchase-intent and financing data without an identifiable Art. 28 processing agreement in AutoScout24's available disclosures

```
adobe_app_id (production): 062a88abff57/c534377b9754/launch-bb13e88bf9a9-development
adobe_app_id (debug):      062a88abff57/c534377b9754/launch-cc5bc64c97e
SDK: com.iterable.iterableapi (marketing CRM)
SDK: api.mediarithmics.com (customer data platform, real-time bidding -- see also C1)
```

Art. 28 processing agreement for the Mediarithmics transfer: asked in writing on 2026-06-30, 2026-08-09, and 2026-08-18; never answered.
 Adobe and Iterable named as processors in AutoScout24's available privacy disclosures: not identified.

Impact: Adobe Experience Platform Launch (both production and debug app IDs compiled into the binary), Iterable's marketing-CRM SDK, and the Mediarithmics customer data platform (also implicated in C1's cleartext finding) all process user behavioral and purchase-intent data – including, for Mediarithmics specifically, financing-intent signals carried over the cleartext connection described in C1. None of the three is identifiably named as a processor for this specific behavioral-data processing in AutoScout24's available privacy disclosures. Which Art. 28 processing agreement governs the transfer of behavioral data to Mediarithmics, and how cleartext transport to a behavioral-data CDP is reconciled with Art. 5(1)(f), was asked directly and never answered.

Impact Analysis

C1 and H1 through H3 share a common thread with C2: each is a decision AutoScout24 made about how to configure transport, credentials, consent timing, or third-party data flows, without the accompanying safeguard or transparency documentation GDPR requires for each specific choice. C1 is the most structurally serious finding in this set – it is not a missing control but a written exception, placed on the exact endpoint that carries financing and income-adjacent data for a platform with 28 million monthly users. H3 compounds C1 directly: the same Mediarithmics CDP implicated in the cleartext exception is also the processor whose Art. 28 agreement was never confirmed. That AutoScout24 ultimately produced two genuine replies – rather than zero – distinguishes this case from others in this campaign: the company is reachable, and a named Senior Legal Counsel engaged with the correspondence. But engagement that corrects a dead mailbox while leaving all four substantive questions unanswered across 96 days and three further deadlines (25 August, 15 September, embargo 28 September) is, functionally, a non-answer on the merits – just one delivered with more care than silence.

The Complete Chain: Ten Messages Across 96 Days, Two Replies and Zero Answers

30 June 2026: RFI-IRFOS sends the original disclosure to security@autoscout24.com and datenschutz@autoscout24.com, CC press@autoscout24.com, the Austrian DSB, CERT.at, and the BayLDA. Embargo fixed: 28 September 2026. datenschutz@autoscout24.com hard-bounces within the hour.

6 July 2026 (6 days): First follow-up. datenschutz@autoscout24.com bounces again.

17 July 2026 (17 days): Second follow-up, yes/no question format, to security@autoscout24.com only.

23 July 2026 and 31 July 2026: Further follow-ups, no reply.

24 July 2026: datenschutz@autoscout24.com bounces a third and final time; dropped from further use.

9 August 2026 (40 days, two messages sent the same morning): Follow-up restating the three original questions in full, noting the campaign now spans 215+ apps at 100+ companies. No reply.

17 August 2026 (49 days): First reply. security@autoscout24.com directs RFI-IRFOS to AutoScout24's Intigriti vulnerability disclosure program.

18 August 2026 (sent twice, 04:42 and 05:05): RFI-IRFOS declines the VDP redirection in detail, restates the findings, adds a fourth question, sets a deadline of 25 August 2026.

20 August 2026: Second reply. Senior Legal Counsel Darko Radonjic states the matter is under review and corrects the data protection address to as24-datenschutz@autoscout24.com. No question answered.

25 August 2026: Deadline passes. No further word.

3 September 2026: RFI-IRFOS's final follow-up, to the expanded recipient list including the corrected address, sets a final deadline of 15 September 2026. An automated customer-service acknowledgment arrives 36 seconds later – not a substantive reply.

15 September 2026: Final deadline passes. No further word.

28 September 2026: Embargo reached. Correspondence record: 10 messages sent by RFI-IRFOS, 3 hard bounces, 2 genuine replies, 0 of 4 questions answered.

17 October 2026: This report publishes, 19 days after embargo, 109 days after original disclosure. All five findings confirmed unaddressed.

Disclosure Timeline & Outcome

2026-06-30 Initial disclosure sent to security@autoscout24.com and datenschutz@autoscout24.com, CC press@autoscout24.com, DSB, CERT.at, BayLDA. Embargo fixed at 2026-09-28. datenschutz@autoscout24.com hard-bounces.

2026-07-06 / 2026-07-17 / 2026-07-23 / 2026-07-31 / 2026-08-09 (x2) Follow-ups sent, 6 through 40 days. datenschutz@autoscout24.com bounces again on 2026-07-06 and 2026-07-24. No reply from security@autoscout24.com.

2026-08-17 First reply: security@autoscout24.com redirects to the Intigriti VDP.

2026-08-18 (x2) RFI-IRFOS declines the redirection, restates findings, sets deadline 2026-08-25.

2026-08-20 Second reply: Senior Legal Counsel Darko Radonjic acknowledges review is underway, corrects the contact address. No question answered.

2026-08-25 Deadline passes, no word.

2026-09-03 Final follow-up sent to expanded recipient list; draws only an automated customer-service acknowledgment.

2026-09-15 Final deadline passes, no word.

2026-09-28 Embargo date reached. Correspondence record: 10 messages sent, 3 hard bounces, 2 genuine replies, 0 questions answered.

2026-10-17 This report published, 19 days after embargo, 109 days after original disclosure. All five findings unaddressed.

Data Protection — Article by Article

Art. 32(1)(a) GDPR – Encryption of personal data: C1's explicit cleartext configuration on a financing endpoint falls short of the state-of-the-art encryption Art. 32(1)(a) requires as an affirmative measure, not a best practice.

Art. 35 GDPR – Data protection impact assessment: C1's combination of financing-intent data and unencrypted transport implicates the DPIA obligation; whether one was conducted was asked four times and never answered.

Art. 32(1)(b) GDPR – Security of processing: C2's hardcoded production Firebase credential implicates the same resilience-of-processing standard.

Art. 7 GDPR – Conditions for consent: H1's pre-consent ContentProvider initializations and H2's boot-time receivers both mean any consent collected later cannot retroactively authorize processing that already began.

Art. 5(1)(c) GDPR – Data minimisation: H2's IMEI access on a financing-intent platform, with no stated purpose, implicates data minimisation directly.

Art. 13 GDPR – Transparency: H2 (IMEI purpose) and H3 (Adobe/Iterable/Mediarithmics as processors) both implicate the obligation to state the specific purpose and recipients of processing.

Art. 28 GDPR – Processor agreements: H3's Mediarithmics, Adobe, and Iterable integrations implicate the requirement for a documented processing agreement; none was identified or confirmed.

Art. 33 GDPR – Notification of a personal data breach to the supervisory authority; Art. 37(7) / Art. 38(1) – DPO contact publication and involvement: the dead datenschutz@autoscout24.com mailbox, live and failing for at least 24 days before being corrected, implicates both the publication requirement for DPO contact details and the requirement that the DPO be involved properly and in a timely manner in matters concerning personal data.

Regulatory Landscape & Fine Exposure

AutoScout24 Engine GmbH and AutoScout24 GmbH are registered in Munich, Germany, placing the company under the jurisdiction of the Bavarian data protection authority (BayLDA) as lead supervisory authority; the Austrian DSB and CERT.at were copied throughout this correspondence, and the BayLDA itself has had full visibility into the exchange, including the dead mailbox and the unanswered questions, since the first message. As a German-registered controller processing financing and behavioral data for roughly 28 million monthly users across the EU, AutoScout24 is subject to GDPR's full Article 83 fine structure.

Art. 83(5) GDPR – Maximum fines up to EUR 20,000,000 or 4% of worldwide annual turnover – applies to violations of Art. 5 (principles), Art. 6 (lawfulness), Art. 7 (consent), and Art. 13 (transparency). H1, H2, and H3 each implicate at least one of these articles.

Art. 83(4) GDPR – Maximum fines up to EUR 10,000,000 or 2% of worldwide annual turnover – applies to violations of Art. 25, Art. 28 (processor agreements), Art. 32 (security of processing), Art. 35 (DPIA), Art. 37, and Art. 38 (DPO obligations). C1, C2, and H3 implicate this tier, as does the dead DPO mailbox itself.

Given AutoScout24's reported valuation exceeding EUR 2.5 billion and its position as Europe's largest car marketplace, the percentage-of-turnover basis for Art. 83(5) is the operative ceiling if any of these findings were to result in an enforcement action by the BayLDA.

Indicators of Compromise

All findings derive from static analysis of com.autoscout24 as published on Google Play, analyzed 2026-06-30 (176.6 MB APK, 96,534 smali classes). No AutoScout24 servers, accounts, or production infrastructure were probed or accessed.

Residual Risk & Recommendations

C1 – Cleartext HTTP on the financing endpoint and Mediarithmics CDP: remove the cleartxtTrafficPermitted exception for rest.autoscout24.com and api.mediarithmics.com, enforce TLS for all EU marketplace domains, and document the Art. 35 DPIA this configuration should have triggered.

C2 – Hardcoded Firebase credentials: rotate the exposed API key, verify Firebase Security Rules independently restrict database access regardless of key exposure, and remove the credential from version-controlled resource files.

H1 – Pre-consent SDK initialization: gate FirebaseInitProvider, MobileAdsInitProvider, and the Adjust lifecycle provider behind a confirmed consent decision rather than ContentProvider auto-init.

H2 – BOOT_COMPLETED + IMEI: document the Art. 6(1) basis for IMEI processing, notify the BayLDA under Art. 33 if not already done, and remove READ_PHONE_STATE if device fingerprinting is not the intended purpose.

H3 – Undisclosed processors: document the Art. 28 agreements governing Adobe, Iterable, and Mediarithmics, and name all three as processors in the privacy policy.

Process-level improvement: datenschutz@autoscout24.com, the address AutoScout24 publishes as its data protection contact, does not accept mail – this should be fixed as a standalone matter independent of this disclosure's substance. A functioning privacy channel that corrects a dead mailbox while still not answering the questions the mailbox exists to receive has fixed the symptom, not the obligation.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736
• Elisabethinergasse 25/10, 8020 Graz, Austria All findings derive from static analysis of

com.autoscout24 as published on Google Play, analyzed 2026-06-30, using publicly available tools (apktool, jadx, jq). No AutoScout24 servers, accounts, or production infrastructure were probed or accessed. Technical evidence is archived under chain of custody and will be provided to the Bayerisches Landesamt für Datenschutzaufsicht (BayLDA) 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 AUTOScout24-2026-R1.