



Security & Privacy Disclosure, Final Report

Chargemap for Android ([com.chargemap_beta.android](https://play.google.com/store/apps/details?id=com.chargemap_beta.android))

An OAuth client secret readable from every install, four hardcoded Google API keys, four SDKs that start before the app's own consent platform, and no network security configuration, shipped unanswered through a 92-day disclosure with zero replies of any kind

**PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 26
SEPTEMBER 2026, FIVE FINDINGS REMAIN UNADDRESSED**

Target	Chargemap
Package	com.chargemap_beta.android
Platform Audited	Android 16 · v4.59.3 (versionCode 100000208), static analysis of the production APK
Initial Disclosure (R1)	2026-06-26 (REF CHARGEMAP-2026)
Disclosure / Embargo Date	2026-09-26
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	5 (4 Critical, 1 High)
Correspondence	9 messages sent by RFI-IRFOS (1 initial disclosure, 8 follow-ups), 0 replies of any kind received, security@chargemap.com and notifications@cnil.fr bounced on every attempt
Authorities BCC'd	Austrian Datenschutzbehoerde (DSB) · French CNIL (bounced) · German BfDI

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: MULTIPLATFORM_CLIENT_SECRET, SINGULAR_SECRET, and a Facebook client token hardcoded in the production binary	7
4.2	C2: Four Google Cloud API keys hardcoded, including a Firebase key exposing the backend project to unauthenticated probing	7
4.3	C3: Four SDKs initialize before Chargemap's own Didomi consent platform loads	8
4.4	C4: No network security configuration, cleartext HTTP permitted by default on a GPS location-tracking app	8
4.5	H1: Useinsider and Mixpanel SDKs receive EV charging movement data without a confirmed Art. 28 processing agreement	9
5	Impact Analysis	9
6	The Complete Chain: From Install to Backend Impersonation and Unencrypted Location Exposure	10
7	Data Protection — Article by Article	11
8	Regulatory & Legal Landscape	11
9	Indicators of Compromise	12
10	Disclosure Timeline & Outcome	13
11	What Chargemap Got Right	14
12	Residual Risk & Recommendations	14

Executive Summary

Chargemap operates a Europe-wide platform for locating electric-vehicle charging stations and paying for charging sessions, used by more than 2.5 million e-drivers across Europe. The Android application manages account identity, payment methods, and the real-time GPS location of every charging session a user starts or searches for.

Static analysis of the production application (v4.59.3) identified five findings. The production binary contains `MULTIPLATFORM_CLIENT_SECRET`, `SINGULAR_SECRET`, and a Facebook client token hardcoded in plain text in `res/values/strings.xml`: a client secret is the private half of an OAuth2 credential pair, and anyone who downloads the app from the Play Store can use it to authenticate as the official Chargemap app directly against Chargemap's own backend. Four Google Cloud API keys (Maps, Places, Static Maps, and Firebase) are hardcoded alongside it, the Firebase key additionally exposing Chargemap's own Firebase project to unauthenticated database probing. Four third-party SDKs, Google Mobile Ads, Firebase Analytics, Google ML Kit, and the Facebook SDK, are declared as Android ContentProviders with a positive `initOrder`, meaning the Android runtime starts them before the first Activity and before any consent screen can appear, ahead of Chargemap's own Didomi consent management platform, so every single install collects data through four separate SDKs before the user has had any opportunity to accept or decline. No network security configuration file exists in the application, so cleartext HTTP traffic is permitted by default, exposing GPS coordinates, session tokens, and account identifiers to interception on any untrusted network. A fifth finding, the Useinsider and Mixpanel SDKs receiving EV charging movement data without a confirmed Art. 28 data processing agreement, corrects to HIGH rather than CRITICAL, a third-party disclosure gap rather than a credential-level failure.

RFI-IRFOS disclosed these findings to privacy@chargemap.com and security@chargemap.com on 26 June 2026 under REF CHARGEMAP-2026, BCC to the Austrian Datenschutzbehörde, the French CNIL, and the German BfDI. security@chargemap.com bounced immediately (550 5.1.1, address not found) and continued to bounce on every subsequent attempt until it was dropped from the thread after the sixth follow-up; notifications@cnil.fr also bounced on the only attempt to use it. Across the following thirteen weeks, RFI-IRFOS sent eight follow-up messages, on 6 July, 17 July, 23 July, 27 July, 5 August, 12 August, 21 August, and 28 August 2026, repeating the same three yes/no questions each time: whether Chargemap's security team was aware the client secret was readable, whether a signed Art. 28 DPA exists with Useinsider, and whether the client secret and consent ordering would be fixed before or after CNIL made contact. Chargemap never once replied, not with an acknowledgment, a rejection, or a bounce-independent message of any kind, across nine messages and ninety-two days. The stated embargo of 26 September 2026 passed three weeks ago; this report, published 21 days after that date, is the first public record of this case.

The coordinated disclosure date was restated as 26 September 2026 in eight of the nine messages sent. One message, sent 17 July 2026, stated 24 September instead; that date was an isolated drafting error, corrected in every message sent before and after it, and 26 September is the date this report treats as authoritative, consistent with the original disclosure and the overwhelming majority of the correspondence.

ID	Severity	Title
C1	CRITICAL	MULTIPLATFORM_CLIENT_SECRET, SINGULAR_SECRET, and a Facebook client token hardcoded in the production binary
C2	CRITICAL	Four Google Cloud API keys hardcoded, including a Firebase key exposing the backend project to unauthenticated probing
C3	CRITICAL	Four SDKs initialize before Chargemap's own Didomi consent platform loads
C4	CRITICAL	No network security configuration, cleartext HTTP permitted by default on a GPS location-tracking app
H1	HIGH	Useinsider and Mixpanel SDKs receive EV charging movement data without a confirmed Art. 28 processing agreement

Subject & Operator Context

Chargemap (Strasbourg, France) operates one of the largest electric-vehicle charging-station platforms in Europe, combining a crowdsourced map of charging points with in-app payment for charging sessions, used by more than 2.5 million e-drivers. The audited application, `com.chargemap_beta.android` (v4.59.3, versionCode 100000208), handles account identity, stored payment methods via Auth0 JWT authentication and the Adapty subscription framework, and continuous GPS location data tied to individual charging sessions.

An EV charging-location app occupies a specific and sensitive position in the GDPR data-minimisation framework: the combination of GPS coordinates, timestamps, and charging-session duration is sufficient to reconstruct a detailed movement profile of a user's daily routine, home location, and commute pattern, data considerably more revealing than the charging transaction itself requires. The findings in this report concern exactly that combination: a credential that lets anyone impersonate the app to its own backend, a consent-ordering defect that lets third-party SDKs collect data before any consent screen appears, and the absence of transport-layer protection for exactly the kind of location data this app is built around.

Engagement Summary

RFI-IRFOS sent the initial disclosure (REF CHARGEMAP-2026) on 26 June 2026 to privacy@chargemap.com and security@chargemap.com, CC contact@chargemap.com and press@chargemap.com, BCC the Austrian DSB, the French CNIL, and the German BfDI. security@chargemap.com bounced immediately (550 5.1.1); notifications@cnil.fr also bounced on this first attempt and was not retried.

RFI-IRFOS followed up eight times over the following thirteen weeks, each restating the open findings and the same three yes/no questions, each met with silence: 6 July 2026 (10 days, zero reply, security@chargemap.com bounced again), 17 July 2026 (21 days, to privacy@chargemap.com only, this message stated the embargo as 24 September in error), 23 July 2026 (28 days, security@chargemap.com bounced a third time, the Austrian DSB added to visible CC), 27 July 2026 (day 21 of the three-questions cycle, the German BfDI added to visible CC), 5 August 2026 (40 days, security@chargemap.com bounced a fourth time), 12 August 2026 (day 47, security@chargemap.com formally dropped from the thread after four consecutive hard bounces, confirming the address does not exist), 21 August 2026 (day 56, zero reply of any kind), and 28 August 2026 (day 63, seven days of silence since the prior message, the eighth follow-up, restating all five findings in full and the stated embargo of 26 September 2026, explicitly correcting the 17 July date error).

No message from Chargemap, human or automated, was ever received in this thread beyond the mail-server bounce notifications for the two dead addresses. No further contact has been sent or received since 28 August 2026. The embargo date of 26 September 2026 passed 21 days before this report's publication date with the case in exactly this state: nine messages sent, zero replies of any kind.

Findings

C1: MULTIPLATFORM_CLIENT_SECRET, SINGULAR_SECRET, and a Facebook client token hardcoded in the production binary

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, 8.5) — OAuth client secret readable from every install, blast-radius escalated from HIGH

```
MULTIPLATFORM_CLIENT_SECRET = 51099a98-445d-4e5e-8811-5f0512924eb2
SINGULAR_SECRET              = 21bbe8c99a7bbe14156698a53e1e3c01
FACEBOOK_CLIENT_TOKEN        = 789ef2ca25234c3d7d4b8f15912b7349
```

Impact: RFI-IRFOS blast-radius escalation: raised from HIGH/8.5 to CRITICAL because MULTIPLATFORM_CLIENT_SECRET = 51099a98-445d-4e5e-8811-5f0512924eb2, extracted directly from res/values/strings.xml in the current Play Store binary, allows any holder of the public APK to authenticate as the official Chargemap app against Chargemap's own backend, without owning a real user device or any Chargemap account. That capability is not confined to a narrow subset of users or a theoretical attacker; it is available to anyone who downloads the app, which is the entire install base. SINGULAR_SECRET = 21bbe8c99a7bbe14156698a53e1e3c01 additionally allows injection of arbitrary fake attribution events into Chargemap's marketing measurement system, and a Facebook client token (789ef2ca25234c3d7d4b8f15912b7349) is exposed alongside both.

C2: Four Google Cloud API keys hardcoded, including a Firebase key exposing the backend project to unauthenticated probing

CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:L/SC:N/SI:N/SA:N, 7.1) — four independently exploitable Google API keys, blast-radius escalated from HIGH

```
GOOGLE_API_KEY_MAPS          = AIzaSyBL-daWpfyax_b_hQKLAP1d1-sn9cSheI
GOOGLE_API_KEY_PLACES        = AIzaSyBlf7Ec9D4h6_nieofUNlhftSE2lflFKec
GOOGLE_API_KEY_STATIC_MAP    = AIzaSyB2CarnGS05F-8zTBgu-Ag1sG0ZZi93MPQ
google_api_key (Firebase)    = AIzaSyA-6Lz145ZfU3ZIyteCPNKuKW0xe9vFoho
```

Impact: RFI-IRFOS blast-radius escalation: raised from HIGH/7.1 to CRITICAL because the Firebase key exposes Chargemap's own Firebase project to unauthenticated database probing in addition to quota-exhaustion risk across three further Google Maps-family keys, and all four sit in the same public binary as C1's client secret, meaning the same single APK extraction yields both a backend-impersonation credential and direct cloud-project access. Each key is independently exploitable; a map-family key enables quota exhaustion against Chargemap's own billing account, while the Firebase key is a direct path to database probing, not merely a cost-denial vector.

C3: Four SDKs initialize before Chargemap's own Didomi consent platform loads

CRITICAL (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, 5.4) — consent-before-processing defeated for every single install, blast-radius escalated from MEDIUM

```
MobileAdsInitProvider  initOrder=100  (Google Mobile Ads)
FirebaseInitProvider  initOrder=100  (Firebase Analytics)
MLKitInitProvider     initOrder=99   (Google ML Kit)
FacebookInitProvider  [auto-init]  (Facebook SDK)

io.didomi.sdk (Didomi CMP) -- loads AFTER all four above
```

Impact: RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.4 to CRITICAL because this is not an intermittent or conditional failure affecting some users: Android starts a ContentProvider with a positive initOrder before the first Activity of any app is shown, before any screen, and therefore before any consent dialog can possibly be presented. All four SDKs below begin collecting data at that point, for every single install without exception, converting an ordering defect into a universal, systemic Art. 7(1) violation rather than an isolated misconfiguration. Chargemap's integration of Didomi as a consent management platform is a deliberate, non-trivial compliance investment; the problem is that it currently governs nothing, because by the time it loads, four SDKs have already started.

C4: No network security configuration, cleartext HTTP permitted by default on a GPS location-tracking app

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, 7.5) — unencrypted transport for GPS, session tokens, and account identifiers, blast-radius escalated from HIGH

```
res/xml/network_security_config.xml : NOT FOUND
Android default (no NSC present): cleartext HTTP traffic permitted
-> GPS coordinates, session tokens, account identifiers
    transmitted unencrypted on any network
```

Impact: RFI-IRFOS blast-radius escalation: raised from HIGH/7.5 to CRITICAL because Chargemap is specifically a GPS-based EV-charging-location app, which means every unencrypted request on an untrusted network exposes exactly the category of data GDPR Art. 32 is designed to protect: which charging station a user is at, at what time, for how long, alongside the session token and account identifier needed to act as that user. No res/xml/network_security_config.xml file was found during this audit; Android's default behaviour at this app's target SDK level permits cleartext HTTP to any host absent such a file. A man-in-the-middle position on a hotel, airport, or public-charging-station Wi-Fi network, precisely the networks a traveling EV driver is likely to be on, is sufficient to intercept this traffic.

H1: Useinsider and Mixpanel SDKs receive EV charging movement data without a confirmed Art. 28 processing agreement

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)
— third-party disclosure gap, corrected from the original audit's CRITICAL working label

com/useinsider/insider/	(Useinsider Inc., Istanbul / San Francisco)
com/mixpanel/android/	(Mixpanel Inc., San Francisco)

Impact: Corrected from the original audit's working CRITICAL label to HIGH: com/useinsider/insider/ (Useinsider Inc., Istanbul and San Francisco) and com/mixpanel/android/ (Mixpanel Inc., San Francisco) are both present in the production binary and positioned to receive GPS coordinates and timing data tied to individual EV charging sessions, a granular movement profile of a user's daily routine, home location, and commute pattern, for behavioural segmentation and marketing automation. As far as this audit can determine, no signed Art. 28 data processing agreement with Useinsider covering this specific data flow is referenced anywhere in Chargemap's available documentation, and both vendors' infrastructure involves data flows outside the EU/EEA, engaging Art. 44 transfer rules. This is a third-party disclosure and processor-agreement gap, not a confirmed exfiltration path comparable to C1 through C4, which is why it is scored and labelled separately from them.

Impact Analysis

C1 through C4 together describe a single production binary from which an attacker can extract: a credential sufficient to impersonate the official app to its own backend (C1), four independently exploitable cloud API keys including one exposing a Firebase project to unauthenticated probing (C2), a consent-platform integration that currently governs nothing because four SDKs start before it loads (C3), and no transport-layer protection at all for the GPS and session data this app is specifically built around (C4). None of these four findings requires any privileged access, device compromise, or social engineering; all four are reachable by decompiling the publicly downloadable APK with freely available tooling.

H1 describes a narrower, but still live, gap: two third-party vendors receiving movement data derived from charging-session location without a confirmed processing agreement. It is scored and treated separately from C1-C4 precisely because it is a disclosure and documentation gap rather than a credential-level or architectural failure, and conflating the two would understate how much more severe C1-C4 are.

The Complete Chain: From Install to Backend Impersonation and Unencrypted Location Exposure

Step 1 — Install: Download Chargemap (com.chargemap_beta.android) from the Google Play Store. No special permissions are required beyond the application's own declared manifest.

Step 2 — Extract: Pull the production APK (v4.59.3, versionCode 100000208) from an enrolled test device via adb, or obtain it directly from Play.

Step 3 — Decompile: Run apktool against the base APK. res/values/strings.xml yields MULTIPLATFORM_CLIENT_SECRET, SINGULAR_SECRET, and the Facebook client token (C1) in plain text, alongside four Google API keys (C2). AndroidManifest.xml reveals the ContentProvider initOrder values for four SDKs that start before Didomi (C3), and the res/xml directory confirms no network_security_config.xml is present (C4).

Step 4 — Backend impersonation: With MULTIPLATFORM_CLIENT_SECRET in hand, any holder of the public binary can request access tokens and call Chargemap's backend APIs as the official app, without owning a real device or account.

Step 5 — Pre-consent data collection: From the moment the app's process starts, before any Activity or consent dialog is shown, Google Mobile Ads, Firebase Analytics, Google ML Kit, and the Facebook SDK have already begun initializing and collecting data, for every install, unconditionally.

Step 6 — Interception: Any session on an untrusted network, a hotel, an airport, or a public charging station's own Wi-Fi, can have its GPS coordinates, session tokens, and account identifiers intercepted in cleartext, because no network security configuration restricts the app to encrypted transport.

By the time a single charging session is located and paid for, Chargemap's own backend authentication, four third-party SDKs' pre-consent data collection, and the session's GPS and payment-adjacent metadata are all structurally exposed, none of it requiring any attacker capability beyond decompiling the public binary and, for C4, sharing a network with the user.

Data Protection — Article by Article

Art. 32 GDPR — Security of processing: C1's hardcoded OAuth client secret, C2's four hardcoded API keys, and C4's absent network security configuration together describe a production application that does not meet the appropriate technical security measures Art. 32 requires for a backend-authentication credential, four independently exploitable cloud keys, and location/session data in transit.

Art. 7(1) GDPR — Conditions for consent: C3's ContentProvider initialization order means consent is structurally collected after processing has already started for four separate SDKs, on every install, the precise condition Art. 7(1) requires consent to precede.

Art. 6(1) GDPR — Lawfulness of processing: the same pre-consent data collection in C3 lacks a lawful basis at the moment processing begins, since the consent mechanism intended to establish one has not yet loaded.

Art. 5(1)(c) GDPR — Data minimisation: H1's transmission of granular EV-charging movement data to Useinsider and Mixpanel for marketing segmentation exceeds what charging-session functionality itself requires.

Art. 13(1)(e) GDPR — Transparency, recipients of data: H1's Useinsider and Mixpanel data flows were not identified as disclosed, Art. 28-covered recipients in documentation available to this audit.

Art. 44 GDPR — Transfers to third countries: Useinsider's Istanbul/San Francisco infrastructure and Mixpanel's San Francisco infrastructure both engage Art. 44 transfer-mechanism requirements for the EV movement data described in H1.

Art. 33(4) GDPR — Notification of a personal data breach: RFI-IRFOS's disclosure placed Chargemap on notice from 26 June 2026 that, to the extent C1's exposed client secret is treated as a personal data breach, the 72-hour notification clock under Art. 33 runs from the date Chargemap became aware, at the latest the date of initial disclosure.

Regulatory & Legal Landscape

Chargemap is a French company operating a platform used across the EU/EEA, placing the French CNIL in the natural lead-supervisory-authority position; RFI-IRFOS BCC'd notification s@cnil.fr on the initial disclosure, which bounced (550 5.1.1) and was not successfully retried in this thread, leaving CNIL without a confirmed direct copy of this disclosure through RFI-IRFOS's own correspondence. The Austrian DSB and the German BfDI were BCC'd throughout as the relevant authorities under Art. 3(2) extraterritorial scope for Chargemap's Austrian and German-resident users.

Fine exposure under GDPR: Art. 83(4) applies to the Art. 5, 6, 7, 13, and 44 violations described in C3 and H1, administrative fines up to EUR 10,000,000 or 2% of total worldwide annual turnover, whichever is higher. Art. 83(5) applies to the Art. 32 security-of-processing failures in C1, C2, and C4, up to EUR 20,000,000 or 4% of total worldwide annual turnover. A hardcoded, backend-impersonating OAuth client secret readable from every install of an app used by more than 2.5 million e-drivers is precisely the category of systemic security failure Art. 32 and Art. 83(5) were designed to address.

Indicators of Compromise

The following identifiers and class names were extracted from the production APK (v4.59.3, versionCode 100000208, audited 2026-06-26) via static analysis only. No Chargemap servers, accounts, or infrastructure were probed.

```
C1 -- Hardcoded secrets (res/values/strings.xml)
MULTIPLATFORM_CLIENT_SECRET = 51099a98-445d-4e5e-8811-5f0512924eb2
SINGULAR_SECRET              = 21bbe8c99a7bbe14156698a53e1e3c01
FACEBOOK_CLIENT_TOKEN        = 789ef2ca25234c3d7d4b8f15912b7349

C2 -- Hardcoded Google API keys
GOOGLE_API_KEY_MAPS, GOOGLE_API_KEY_PLACES,
GOOGLE_API_KEY_STATIC_MAP, google_api_key (Firebase)

C3 -- Pre-consent ContentProviders (AndroidManifest.xml)
MobileAdsInitProvider, FirebaseInitProvider,
MlKitInitProvider, FacebookInitProvider
(all load before io.didomi.sdk)

C4 -- Missing configuration
res/xml/network_security_config.xml : NOT FOUND

H1 -- Third-party SDK packages
com/useinsider/insider/, com/mixpanel/android/
```

Disclosure Timeline & Outcome

2026-06-26 Initial disclosure (R1, REF CHARGEMAP-2026) sent to privacy@chargemap.com and security@chargemap.com. CC: contact@chargemap.com, press@chargemap.com. BCC: Austrian DSB, French CNIL, German BfDI. security@chargemap.com and notifications@cnil.fr both bounce immediately (550 5.1.1, address not found).

2026-07-06 Follow-up #1, 10 days, zero reply. security@chargemap.com bounces again.

2026-07-17 Follow-up #2, 21 days. Sent to privacy@chargemap.com only. This message states the embargo date as 24 September 2026, a drafting error later corrected.

2026-07-23 Follow-up #3, 28 days. security@chargemap.com bounces a third time. Austrian DSB added to visible CC.

2026-07-27 Follow-up #4, day 21 of the three-questions cycle. German BfDI added to visible CC alongside the DSB.

2026-08-05 Follow-up #5 (sent 2026-08-04 22:08 UTC), 40 days, zero reply of any kind. security@chargemap.com bounces a fourth time.

2026-08-12 Follow-up #6, day 47. security@chargemap.com formally dropped from the thread after four consecutive hard bounces confirming the address does not exist; privacy@chargemap.com remains the only address in this thread that has ever accepted delivery.

2026-08-21 Follow-up #7, day 56, zero reply of any kind.

2026-08-28 Follow-up #8 (the eighth follow-up, ninth message overall), day 63, seven days of silence since the prior message. Restates all five findings in full and explicitly reconfirms the embargo date as 26 September 2026, correcting the 17 July error.

2026-09-26 Stated embargo date reached. No message of any kind, human or automated beyond the two address-bounce notifications already received, has been sent by Chargemap at any point in this thread.

2026-10-17 This report published, 21 days after the embargo date. All five findings confirmed unaddressed on the basis of the correspondence record; no re-verification download was performed for this report.

What Chargemap Got Right

Chargemap has already invested in a consent management platform (Didomi), Auth0 JWT for authentication, and a structured in-app subscription architecture (Adapty), deliberate, non-trivial compliance and architecture decisions. The problem identified in C3 is not that Didomi was chosen, it is that four SDKs initialize before Didomi can act, a solvable ordering problem rather than an absence of compliance investment.

This does not offset the findings in this report. Choosing a consent platform does not establish that it functions as a gate (C3), and an architecturally sound authentication framework for user-facing login (Auth0) does not substitute for protecting the separate OAuth client secret that authenticates the app itself to its own backend (C1).

Residual Risk & Recommendations

C1 — Immediate: Rotate MULTIPLATFORM_CLIENT_SECRET, SINGULAR_SECRET, and the Facebook client token immediately; none of the three should ever be shipped in a client-side binary. Move backend authentication to a server-side exchange that does not require embedding a long-lived secret in a publicly distributable APK.

C2 — Immediate: Rotate all four Google API keys and apply package-name and SHA-1 certificate restrictions to each one at minimum; apply Firebase Security Rules to close the unauthenticated database-probing path independently of key rotation.

C3 — Immediate: Reorder SDK initialization so that Google Mobile Ads, Firebase Analytics, Google ML Kit, and the Facebook SDK all wait on Didomi's consent signal before any ContentProvider-driven auto-initialization occurs; this is a manifest-level fix, not a redesign.

C4 — Immediate: Add a network_security_config.xml that disables cleartext traffic for all domains Chargemap's backend serves, and verify no fallback path permits plain HTTP for GPS, session-token, or account-identifier traffic.

H1 — Governance: Confirm and document a signed Art. 28 DPA with Useinsider covering the EV charging movement data identified in this report, or remove the data flow if no such agreement exists; document the Art. 44 transfer mechanism relied on for both Useinsider and Mixpanel.

Across all findings: establish a monitored intake address for security and privacy disclosures that does not silently drop messages (security@chargemap.com hard-bounced on every attempt across this entire disclosure), and ensure a human response, even a brief acknowledgment, reaches a disclosure of this severity within a reasonable window rather than the complete silence recorded in this case.

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 root-level analysis of

the published application using publicly available tooling. No Chargemap 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 CHARGEMAP-2026.