Coordinated Security & Privacy Disclosure, Final Report

LinkedIn Android (com.linkedin.android)

LinkedIn Ireland Unlimited Company, a Microsoft Corporation subsidiary (NYSE: MSFT)

CS-DEFLECT · CASE CLOSED AND PUBLISHED 24 SEPTEMBER 2026, 93 DAYS AFTER DISCLOSURE, FIVE DEFLECTION LAYERS, ZERO HUMAN ENGAGEMENT WITH ANY FINDING

Target	LinkedIn Android, the world's largest professional network, over 950 million members
Package	com.linkedin.android
Operator	LinkedIn Ireland Unlimited Company, EU-established data controller, Microsoft Corporation subsidiary
Lead Supervisory Authority	Irish Data Protection Commission (GDPR Art. 56)
Initial Disclosure	2026-06-23
Original Embargo	2026-09-22 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-24, two days after the embargo, an internal publishing gap, not a change in terms
Regulators in BCC	Irish DPC, Austrian DSB, EDPS, German BfDI
Deflection Layers	Five, each named for the record: a customer-service satisfaction survey, two HackerOne portal redirects, an account-support ticket treating a GDPR disclosure as a login problem, and a legal-inbox auto-reply asking not to be contacted again

rfi.irfos@gmail.com • rfi-irfos.com
ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 23 June 2026, RFI-IRFOS disclosed to LinkedIn Ireland Unlimited Company that the LinkedIn Android production binary, distributed to European users via Google Play, contains three hardcoded Chinese tracking endpoints (linkedin.cn, linkedin-ei.cn, linkedin-ei2.cn) compiled into the behavioral telemetry dispatch pipeline, active host-resolution paths with no EU adequacy decision covering the destination and no disclosure of China as a data destination in LinkedIn's privacy policy. Separately, a fully initialized Facebook SDK auto-logs professional behavioral events, which job listings a user opens, how long they spend on recruiter profiles, which companies they follow, to Meta's servers, with AutoLogAppEventsEnabled left at its default of enabled and Facebook never named as a recipient in the privacy policy.

A third finding documented 18 ActivityAlias entries in the manifest corresponding to specific cultural and religious events (Diwali, Lunar New Year, Indian Independence Day, among others), a mechanism capable of inferring and acting on a user's cultural or ethnic identity, itself GDPR Art. 9 special-category data, undisclosed as a processing purpose. A fourth, lower-severity finding documented hardcoded Google API and Firebase project credentials in the production binary.

Across 93 days and multiple outbound messages, every LinkedIn response was a deflection, not an engagement, five distinct patterns in total: (1) an automated customer-service satisfaction survey referencing the disclosure's own case number, (2) and (3) two separate redirects to LinkedIn's HackerOne bug-bounty portal, a channel for a different genre of submission than a formal regulatory disclosure, (4) an account-support ticket that treated the GDPR disclosure as a personal login problem and requested screenshots, and (5) an auto-reply from the legal inbox, itself CC'd on the original disclosure, stating it does not handle this type of request and asking not to be contacted at that address again. No human respondent with GDPR competence engaged a single finding at any point.

All four findings were re-scored under CVSS v4.0 for this closure report, not carried forward with the original hand-assigned labels. C1 (the Chinese tracking endpoints) and C2 (Facebook auto-logging) each have a CVSS v4.0 base of MEDIUM, 6.9, and are held at HIGH in this report under explicit blast-radius escalations, documented in each finding, for a population of 950 million-plus members and, for C1 specifically, a standing PRC National Intelligence Law exposure the technical vector alone does not capture. H1 and M1 correct down to MEDIUM, matching their own CVSS v4.0 bands honestly.

Scope: Root-level static analysis of the production LinkedIn Android application (com.linkedin.android), covering the AndroidManifest, resource strings, and decompiled dex, as pulled and reviewed on 23 June 2026. No dynamic instrumentation, live traffic capture, or interaction with LinkedIn's or Microsoft's backend infrastructure was performed. RFI-IRFOS was unable to pull a fresh production build for this closure report and does not claim to know whether the four findings still hold against the current Google Play build, that gap is stated here explicitly, it is not assumed either way.

Disposition

Four findings were disclosed on 23 June 2026: two CRITICAL (three hardcoded Chinese tracking endpoints compiled into the EU-distributed production binary's behavioral telemetry pipeline, and a fully initialized Facebook SDK auto-logging professional behavioral events with no legal basis or disclosure), one HIGH (18 undisclosed cultural and religious identity profiling activity aliases), and one MEDIUM (hardcoded Google/Firebase API credentials). Across 93 days, LinkedIn's only responses were five distinct deflection layers, none of which engaged a single finding: a customer-service satisfaction survey, two redirects to the HackerOne bug-bounty portal, an account-support ticket requesting login screenshots, and a legal-inbox auto-reply stating the address does not handle this type of request and asking not to be contacted again. This report closes and publishes the case on the terms disclosed from the first message.

ID	Severity	Title
C1	HIGH	Three Hardcoded Chinese Tracking Endpoints in the EU-Distributed Behavioral Telemetry Pipeline
C2	HIGH	Facebook SDK Auto-Logs Professional Behavioral Events With No Legal Basis or Disclosure
H1	MEDIUM	18 Undisclosed Cultural and Religious Identity Profiling Activity Aliases
M1	MEDIUM	Hardcoded Google API Key and Firebase Project Credentials

Subject & Operator Analysis

LinkedIn is the world's largest professional network, over 950 million members, operated by LinkedIn Ireland Unlimited Company, an EU-established data controller and a Microsoft Corporation subsidiary. The Irish Data Protection Commission is LinkedIn Ireland's lead supervisory authority under GDPR Art. 56. Several genuine positives are worth naming: allowBackup is set to false, the permission scope is narrow (no camera, no contacts, no precise location), and the network security configuration provides a clean default without cleartext-traffic exceptions for arbitrary domains, meaningful engineering decisions that stand alongside the findings below.

This case is a clean, fully documented instance of the automated-deflection pattern this campaign tracks closely: a formal, regulator-BCC'd GDPR disclosure was met with five successive redirect mechanisms across 93 days, never once reaching a person with GDPR competence.

Architecture & Data Flow

The LinkedIn Android production binary compiles a conditional Chinese-endpoint switch into its core behavioral telemetry dispatch pipeline, ships a fully initialized Facebook SDK auto-logging professional activity by default, declares 18 cultural and religious identity-linked activity aliases, and carries hardcoded Google and Firebase project credentials, all inside the same binary served to the entire EU membership via Google Play.

Findings

C1: Three Hardcoded Chinese Tracking Endpoints in the EU-Distributed Behavioral Telemetry Pipeline

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the same binary carrying these compiled endpoints is distributed to LinkedIn's entire 950 million-plus membership through the standard EU Google Play channel, and China's National Intelligence Law Art. 7 exposure is a standing governance fact the technical vector alone does not express.

com/linkedin/android/litrackinglib/network/MetricQueue.smali contains three hardcoded endpoints forming a conditional switch in the behavioral telemetry dispatch pipeline: linkedin.cn/li/track, linkedin-ei2.cn/li/track, and linkedin-ei.cn/li/track, active host-resolution paths compiled into the EU-distributed production binary. China has no GDPR adequacy decision, and LinkedIn's privacy policy does not disclose China as a data transfer destination or recipient anywhere. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the same binary carrying these compiled endpoints is distributed to LinkedIn's entire 950 million-plus membership through the standard EU Google Play channel, and China's National Intelligence Law Art. 7 exposure is a standing governance fact the technical vector alone does not express.

```
smali_classes4/com/linkedin/android/litrackinglib/network/MetricQueue.smali:
:pswitch_1  const-string/jumbo v1, "https://www.linkedin.cn/li/track"
:pswitch_2  const-string/jumbo v1, "https://www.linkedin-ei2.cn/li/track"
:pswitch_3  const-string/jumbo v1, "https://www.linkedin-ei.cn/li/track"

com/linkedin/android/tos/Host$EnumUnboxingLocalUtility.smali:
host resolution enum includes linkedin.cn, linkedin-ei.cn, linkedin-ei2.cn
```

Impact: Behavioral telemetry from EU members can be dispatched to infrastructure operated under Chinese law, a jurisdiction with no EU adequacy decision, compiled into every copy of the binary distributed via Google Play, without any transfer disclosure in LinkedIn's privacy policy.

Fix: Remove the Chinese host resolution paths from the EU-distributed build, or publish the specific Art. 44 transfer mechanism and a transfer impact assessment accounting for NSL Art. 7 obligations. No confirmation that either has occurred was ever received.

C2: Facebook SDK Auto-Logs Professional Behavioral Events With No Legal Basis or Disclosure

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because of the scale, 950 million-plus members, and because the specific data category, professional behavioral signal, flows undisclosed to a competing commercial platform.

The production binary ships a fully initialized Facebook SDK with hardcoded facebook_app_id and facebook_client_token. AutoLogAppEventsEnabled is never set to false anywhere in the binary, the SDK defaults to enabled, and is actively called from at least nine locations across the login and event-logging code paths. In LinkedIn specifically, this means which job listings a user opens, how long they spend on recruiter profiles, which companies they follow, and how often they message, flows to Meta's servers. Facebook is not named as a data recipient in LinkedIn's privacy policy, which refers only to unnamed "service providers." RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because of the scale, 950 million-plus members, and because the specific data category, professional behavioral signal, flows undisclosed to a competing commercial platform.

```
res/values/strings.xml: facebook_app_id, facebook_client_token (hardcoded)
getAutoLogAppEventsEnabled() actively called in:
com/facebook/FacebookSdk.smali, AppEventsLoggerImpl.smali,
InternalAppEventsLogger.smali, LoginMethodHandler.smali, DeviceAuthDialog.smali
```

Impact: The exact professional-behavioral signal LinkedIn itself sells to recruiters and advertisers flows to a separate, competing commercial platform, undisclosed, with no stated Art. 6 legal basis.

Fix: Set AutoLogAppEventsEnabled to false by default, require explicit opt-in, and name Meta Platforms specifically as a data recipient in the privacy policy. No confirmation that any of this has occurred was ever received.

H1: 18 Undisclosed Cultural and Religious Identity Profiling Activity Aliases

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9. Corrected from the original HIGH label under CVSS v4.0, the mechanism's actual use beyond icon-variant selection was not independently confirmed.

The Android manifest declares 18 ActivityAlias entries, each tied to a specific cultural or religious event: Diwali, Lunar New Year, Indian Independence Day, among others. This mechanism is capable of inferring and acting on cultural or ethnic identity signals, GDPR Art. 9 special-category data, undisclosed as a processing purpose anywhere in LinkedIn's privacy policy. RFI-IRFOS's static analysis confirms the aliases exist and are wired into the manifest; it does not independently confirm what runtime signal selects between them or how far that inference is used beyond serving a different icon variant.

```
AndroidManifest.xml, 18 ActivityAlias entries including:
DiwaliActivityAlias, LunarNewYearActivityAlias, IndianIndependenceActivityAlias,
EarthFestivalActivityAlias, WinterFestivalActivityAlias, IntlWomensDayActivityAlias
```

Impact: A mechanism capable of inferring special-category identity signals exists in the binary and is undisclosed as a processing purpose, with the full extent of its runtime use not independently confirmed from static analysis alone.

Fix: Disclose the alias mechanism's actual selection logic and confirm whether it uses inferred cultural or ethnic signals, or only explicit, user-provided locale and calendar settings. No confirmation of either was ever received.

M1: Hardcoded Google API Key and Firebase Project Credentials

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N, 6.9.

res/values/strings.xml contains a hardcoded Google API key, Firebase app ID, and default web client ID, extractable by anyone with access to the publicly distributed APK.

Impact: Standard quota-exhaustion and project-enumeration risk against LinkedIn's Firebase project, no further access confirmed.

Fix: Apply standard key restrictions (package name, signing certificate binding). No confirmation that this has occurred was ever received.

Five Deflection Layers, Named for the Record

#	Layer	What Happened
1	Customer Service Redirect	A formal GDPR Art. 44 disclosure routed to customer service; the reply five days later was an automated satisfaction survey referencing the disclosure's own case number, asking how things went with the service team.
2	HackerOne Redirect (first)	An automated reply pointing formal researchers to LinkedIn's HackerOne bug-bounty program, a channel for a different submission genre than a regulator-BCC'd legal disclosure.
3	HackerOne Redirect (second)	The identical redirect repeated on a subsequent follow-up, unchanged.
4	Account Support Ticket	A formal GDPR disclosure treated as a personal account or login issue, with screenshots requested.
5	Legal Inbox Auto-Deflect	The legal@linkedin.com address, itself CC'd on the original disclosure, auto-replied that the inbox does not handle this type of request and asked not to be contacted there again.

Five distinct mechanisms, five different departments or systems, and not one of them engaged a single one of the four findings. This is documented in the RFI-IRFOS Corporate Response Pattern Atlas v0.1 as a compound instance of the Webform Shuffle (P-01) and Support Ticket Downgrade (P-07) pattern family, repeated across five separate channels in a single case, the most layered deflection RFI-IRFOS has recorded against a single disclosure this campaign.

Data Protection, Article by Article

The findings map onto a small, specific set of GDPR provisions, set out below in one place instead of scattered across the findings themselves.

Article	Finding	Basis
Art. 44, Art. 13(1)(f)	C1	International transfer of behavioral telemetry to infrastructure operated under Chinese law, undisclosed as a transfer destination.
Art. 13(1)(e), Art. 6(1)	C2	Facebook not named as a data recipient; no disclosed legal basis for the transfer of professional behavioral data.
Art. 9(1), Art. 13(1)(c)	H1	Cultural and ethnic identity inference is special-category data, undisclosed as a processing purpose.
Art. 33(1)	General	A 72-hour breach-notification window opened on the original disclosure date; LinkedIn never confirmed, when directly asked, whether the Irish DPC was notified or which Art. 33(3) exception it relied on instead.

Regulatory & Legal Landscape

LinkedIn Ireland Unlimited Company is the EU-established data controller, with the Irish Data Protection Commission as lead supervisory authority under GDPR Art. 56. Microsoft Corporation is LinkedIn's ultimate parent; GDPR Art. 44 recognizes no exception for a US-headquartered parent company. The Austrian DSB, EDPS, and German BfDI were held in BCC across this case's correspondence.

IOC / Reproducible Evidence

```
Package: com.linkedin.android
C1: smali_classes4/com/linkedin/android/litrackinglib/network/MetricQueue.smali
    linkedin.cn, linkedin-ei.cn, linkedin-ei2.cn (/li/track)
C2: res/values/strings.xml facebook_app_id, facebook_client_token
    AutoLogAppEventsEnabled default (never set false)
H1: AndroidManifest.xml, 18 ActivityAlias entries
M1: res/values/strings.xml google_api_key, google_app_id, default_web_client_id
```

No fresh production build was pulled for this closure report. RFI-IRFOS does not claim to know whether the current Google Play build still matches the one reviewed on 23 June 2026, and states that gap explicitly instead of assuming continuity.

Disclosure Timeline & Outcome

Date	Event
2026-06-23	R1 sent to privacy@linkedin.com, cc legal@linkedin.com, security@linkedin.com, privacy@microsoft.com (bounced). Four findings, 90-day embargo set for 2026-09-22.
2026-06-28	Deflection layer 1: customer-service satisfaction survey.
2026-07-07	Deflection layer 2: HackerOne redirect.
2026-07-08	Deflection layer 4: legal-inbox auto-deflect, first instance.
2026-07-23	Deflection layer 4 repeated, unchanged.
2026-07-31	Deflection layers 3 and 5: second HackerOne redirect, and a formal note naming all five layers for the record.
2026-09-22	Original 90-day embargo elapses. No human GDPR-competent reply had ever been received.

Date	Event
2026-09-24	Case closed and published, two days after embargo, on the terms stated from the first message.

Five distinct deflection mechanisms, zero human engagement with any of the four findings, across 93 days.

Residual Risk & Recommendations

All four findings remain unconfirmed as fixed at the time of publication, because no LinkedIn respondent with GDPR competence ever engaged with them. RFI-IRFOS recommends, in order of urgency: remove or properly transfer-safeguard the Chinese telemetry endpoints (C1); disable Facebook AutoLog by default and disclose Meta as a recipient (C2); publish the actual selection logic behind the 18 cultural activity aliases (H1); and apply standard key restrictions to the hardcoded Firebase credentials (M1). Weekly monitoring of the public build continues after this publication; any change to any of the four findings will be documented and added to the public record.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria CVSS v4.0 is RFI-IRFOS's scoring guideline, not a ceiling or a floor. It gives a reproducible, third-party-legible starting point for severity, and it does not capture real-world blast radius on its own, factors such as user population size, a vulnerable or protected class of users, or a standing corporate governance exposure the technical vector alone cannot express. RFI-IRFOS reserves the right to weigh that blast radius above the bare CVSS score, and, more rarely, to hold a score below what CVSS alone would suggest when the underlying claim is unconfirmed or disputed with evidence. Any such escalation is always stated explicitly in the finding itself, never left implicit, as C1 and C2 are escalated and H1 is corrected down in this report. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF LINKEDIN-2026-R1.