Coordinated Security & Privacy Disclosure, Final Report

EY Android app portfolio (seven apps, including EY Interact Payroll com.ey.eyinteractpayroll v26.0.3)

Six written notices, ninety days, two named-team replies, one unsubstantiated self-declared closure, zero further engagement

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – BOTH FINDINGS UNADDRESSED AFTER A CASE EY DECLARED CLOSED WITHOUT TECHNICAL SUBSTANTIATION

Target	Ernst & Young, LLP / EY
Product audited	EY Android app portfolio: EY Interact Payroll, EY Global One, EY Tax & Law, Disprz/EY Learning, EY Meetings, EY Events, EY Virtual Events (seven apps total)
Disclosure reference	REF EY-ANDRD-2026-06-21
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2 dead certificate pinning combined with a deprecated OAuth2 implicit grant on the payroll app, CVSS v4.0 9.3, self-declared closed without substantiation)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of seven EY Android applications and identified two CRITICAL findings: live Firebase API keys hardcoded verbatim across five of the seven production APKs, including EY Interact Payroll, whose exposed project allows unauthenticated Remote Config read and project enumeration against a database backing salary, gross/net pay, tax code, and deduction data, and, on that same payroll app, a certificate-pinning configuration that specifies a valid SHA-256 pin only for a staging domain while the production manifest never references it, combined with an OAuth2 implicit grant authentication flow deprecated by RFC 8252 (2017) and formally superseded by RFC 9700 (2025) for native applications.

cybersecurity@ey.com acknowledged the disclosure on 22 June, and responsible.disclosure@ey.com replied on 28 June declaring the matter closed, stating that 'mitigating controls and proper service configurations have been confirmed which address the observations shared,' without naming which controls, which configurations, or supplying any technical detail capable of independent verification. RFI-IRFOS disputed the closure the same day and sent five further written notices over the following eleven weeks, on 5 August, 15 August, 24 August, 31 August, and 12 September, restating both findings and three outstanding questions on Art. 32 compliance verification, Art. 33 breach notification, and DPIA coverage. None of the five received any further reply from EY.

Scope: Static analysis of the publicly downloaded production APKs for seven EY-branded Android applications, on an authorized test device, only. No EY account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to privacy@ey.com (bounced, address not found) and ey@at.ey.com (delivered), cc security@ey.com, datenschutz@de.ey.com, bcc/cc the Austrian Datenschutzbehoerde, CERT.at, and the German BfDI (bounced). cybersecurity@ey.com acknowledged receipt on 22 June, and responsible.disclosure@ey.com unilaterally declared the case closed on 28 June, stating that 'mitigating controls and proper service configurations have been confirmed' without supplying any supporting technical detail. RFI-IRFOS pushed back the same day and sent five further written notices over the following eleven weeks; none received any further reply.

ID	Severity	Title
C1	CRITICAL	Firebase API keys hardcoded in five of seven production APKs across the EY Android portfolio
C2	CRITICAL	Dead certificate pinning combined with a deprecated OAuth2 implicit grant on the payroll app

Subject & Operator Analysis

Ernst & Young, LLP (EY) is a multinational professional services firm. The seven audited apps span payroll, learning, meetings, events, and tax/law functions across EY's Android app portfolio.

Findings

C1: Firebase API keys hardcoded in five of seven production APKs across the EY Android portfolio

HIGH, 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, 8.8

Live Firebase API keys are embedded verbatim in Play Store binaries for EY Interact Payroll (project eyipnov2024), Disprz/EY Learning (disprztwo), EY Meetings (nth-drive-91717), EY Events (ah-mc-shared-production-eu), and EY Virtual Events (spotme-firebase, third-party SpotMe vendor infrastructure). The payroll app's key exposes a project backing salary, gross/net pay, tax code, and deduction data, and all five keys allow unauthenticated Remote Config read and project enumeration.

EY's 28 June closure message did not name this finding, any of the five affected apps, or any specific remediation step taken against it.

Impact: Payroll and other employee-facing project configuration, including a project backing salary data, can be enumerated and read by any party extracting the corresponding key from the public APK.

Fix: Rotate all five exposed keys, confirm Remote Config and Firestore/RTDB rules are deny-by-default for each project, and enforce App Check.

C2: Dead certificate pinning combined with a deprecated OAuth2 implicit grant on the payroll app

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 9.3

EY Interact Payroll's network_security_config.xml contains a valid SHA-256 certificate pin, but only for a staging domain; the production AndroidManifest.xml never references android:networkSecurityConfig, so pinning is never applied to production traffic against interactpayroll.ey.com. The app authenticates using the OAuth2 implicit grant (response_type=token), deprecated by RFC 8252 in 2017 and formally superseded by RFC 9700 in 2025 for native applications specifically because access tokens returned via URL fragment are exposed to interception and logging.

EY's 28 June closure message did not name this finding or either of its two components, and supplied no evidence that certificate pinning was extended to the production domain or that the authentication flow was migrated to authorization code with PKCE.

Impact: Payroll authentication tokens and traffic are exposed to interception on production infrastructure with no certificate pinning and a token-issuance flow the relevant standards body has deprecated specifically for native apps.

Fix: Apply the existing certificate pin to the production domain via the manifest's networkSecurityConfig reference, and migrate authentication to OAuth2 authorization code with PKCE.

A Case EY Declared Closed Without Naming What Was Fixed

responsible.disclosure@ey.com's 28 June message read in full: 'Upon review through our internal process, mitigating controls and proper service configurations have been confirmed which address the observations shared. As such we consider this matter closed without further engagement.' It named no specific control, no specific app among the five affected, and no verification method. RFI-IRFOS disputed the closure the same day and asked EY to confirm which of the five hardcoded Firebase keys had been rotated and whether the payroll app's certificate-pinning and OAuth2 flow had actually changed. Five further written notices over the following eleven weeks restated this request; none received a reply of any kind.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 25(1), Art. 32(1)(b)	Hardcoded Firebase keys across five production apps, including a payroll project
C2	GDPR Art. 32(1)(a)	No production certificate pinning combined with a deprecated OAuth2 token-issuance flow on a payroll app

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to privacy@ey.com (bounced) and ey@at.ey.com (delivered); 2 CRITICAL findings across 7 apps
2026-06-22	cybersecurity@ey.com acknowledges receipt, no ticket number, no named contact
2026-06-28	responsible.disclosure@ey.com declares the case closed, citing unnamed 'mitigating controls'; RFI-IRFOS disputes the closure the same day
2026-08-24	Follow-up invokes the Art. 33(4) 72-hour breach-notification clock
2026-08-31	Follow-up states audited apps are diffed weekly against the archive; notes a self-declared closure without substantive reply does not stop the embargo clock
2026-09-12	Follow-up restates the full chronology and three unanswered questions, deadline 19 September for a written answer
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Name the specific remediation taken for each of the two findings, rather than an unsubstantiated general closure statement.
- Rotate all five exposed Firebase keys and confirm deny-by-default access rules for each project.
- Apply certificate pinning to the payroll app’s production domain and migrate its authentication flow to authorization code with PKCE.
- Confirm whether an Art. 33 breach notification was made for the payroll findings and, if not, document why none was required.

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 Coordinated disclosure per ISO/IEC 29147. GDPR Art. 25, 32, 33. REF EY-ANDRD-2026-06-21.