Coordinated Security & Privacy Disclosure, Final Report

BAWAG for Android (com.bawagpsk.bawagpsk)

Twelve written notices, seventy-nine days, one automated receipt confirmation, zero substantive replies

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL FIVE FINDINGS UNADDRESSED AFTER TWELVE NOTICES

Target	BAWAG P.S.K. Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG, Vienna, Austria
Product audited	BAWAG for Android, com.bawagpsk.bawagpsk, v3.27.1
Disclosure reference	REF BAWAG-2026-R1
R1 sent	2026-06-25
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	HIGH (H3 Usabilla screenshot SDK on a banking app, CVSS v4.0 7.1, unaddressed)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 25 June 2026, RFI-IRFOS performed static analysis of the production BAWAG Android banking application and identified three HIGH and two MEDIUM findings: an advertising-ID and attribution stack running with no detectable consent-management platform, a Firebase project key extractable from the shipped APK, a third-party feedback SDK with screenshot capability capable of capturing account balances or IBANs to a US recipient, an undocumented biometric and identity-verification stack (FaceTec, IDnow, Microblink) raising Art. 9 and Art. 44 disclosure questions, and a full set of development/staging identity-verification hostnames hardcoded alongside production hosts in the shipped binary.

Across twelve written notices over seventy-nine days, cc'd throughout to the Austrian Datenschutzbehörde and the European Data Protection Supervisor, the only inbound message of any kind in this case was a single fully automated receipt confirmation received on the day R1 was sent, explicitly instructing RFI-IRFOS not to reply to it. No named Data Protection Officer was ever identified, despite R1 explicitly requesting one, and none of RFI-IRFOS's three standing questions, DPO awareness of the consent gap, the existence of Art. 28 processing agreements with Google, Usabilla/Momentive, and FaceTec, and whether any remediation occurred before or after this disclosure, ever received a reply.

A separate but related case against PayLife SESAM (at.paylife.sesam), which R1's own evidence establishes runs on the same underlying BAWAG P.S.K. banking codebase under a different brand, was opened on 6 July 2026 under its own reference and carries its own later embargo of 4 October 2026. That case is not yet due and is not covered by this report; it will be reported separately on its own embargo date.

Scope: Static analysis of the publicly downloaded production BAWAG Android APK (v3.27.1), on an authorized test device, only. No BAWAG account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 25 June 2026 to datenschutz@bawagpsk.com and datenschutz@bawag.at, cc kundenservice@bawagpsk.com, communications@bawaggroup.com, stop-phishing@bawag.at, investor.relations@bawaggroup.com, and from 3 July onward the Austrian DSB and EDPS. Across twelve written notices over seventy-nine days, the only inbound message of any kind was a single fully automated receipt confirmation on the day R1 was sent. No named Art. 37 DPO, no substantive reply, and no acknowledgment of any finding was ever received.

ID	Severity	Title
H1	HIGH	Advertising ID and attribution stack with no detectable consent-management platform
H2	HIGH	Firebase project key and configuration extractable from the public APK
H3	HIGH	Usabilla feedback SDK with screenshot capability on a banking app

ID	Severity	Title
M1	MEDIUM	Biometric and identity-verification stack, disclosure and transfer question
M2	MEDIUM	Development and staging identity-verification hosts hardcoded in the production binary

Subject & Operator Analysis

BAWAG P.S.K. Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG operates as part of BAWAG Group AG, headquartered in Vienna, Austria, under the direct jurisdiction of the Austrian Datenschutzbehörde.

Findings

H1: Advertising ID and attribution stack with no detectable consent-management platform

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

ACCESS_ADSERVICES_AD_ID and ACCESS_ADSERVICES_ATTRIBUTION permissions declared, with the com.google.android.gms.ads_identifier SDK bundled. No recognized consent-management platform, Usercentrics, OneTrust, Didomi, or Sourcepoint, was found in the binary.

No reply of any kind, substantive or otherwise, addressed this finding across twelve notices.

Impact: Advertising-identifier processing on a banking app operates without a demonstrable lawful-basis consent gate.

Fix: Deploy a recognized consent-management platform gating AD_ID collection, or remove the advertising-identifier permissions if unused.

H2: Firebase project key and configuration extractable from the public APK

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

project_id bawag-prod-android and google_api_key AIzaSyDIoUyTN9IXemN863U9sd6MW6MGIPDqtIE, both extractable from the shipped APK.

Risk depends on whether Firestore rules are deny-by-default and App Check is enforced, neither of which RFI-IRFOS can verify externally: quota/billing denial-of-service, direct read/write access if rules are permissive, or replay if App Check is absent. No reply of any kind addressed this finding.

Impact: A production Firebase project's attack surface cannot be independently ruled safe from outside the console.

Fix: Confirm and publish that Firestore security rules are deny-by-default and App Check is enforced for this project.

H3: Usabilla feedback SDK with screenshot capability on a banking app

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 7.1

com.usabilla.sdk.ubform.screenshot.UbScreenshotActivity (Usabilla/Momentive, a US feedback platform) can attach a screenshot to a feedback submission.

On a banking app, a feedback-attached screenshot could capture account balances, transactions, or IBANs, transmitted to a US third party. No reply of any kind addressed this finding.

Impact: A user submitting feedback from within the app risks transmitting visible account or transaction data to a third-party US platform without a specific warning at the point of capture.

Fix: Restrict the screenshot attachment to explicitly-drawn UI regions, or remove the capability, and disclose the Usabilla/Momentive data transfer explicitly.

M1: Biometric and identity-verification stack, disclosure and transfer question

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

com.facetec.sdk (FaceTec, US, 3D face biometric), de.idnow (IDnow, KYC), and com.microblink.photopay (document/payment-slip OCR) are present.

This finding is about disclosure, not the legitimacy of KYC verification itself: FaceTec processes Art. 9 special-category biometric data with a US recipient under Art. 44, and RFI-IRFOS asked whether these processors and transfers are named in the app's privacy information under Art. 13(1)(e). No reply of any kind answered this question.

Impact: Special-category biometric processing and a US data transfer may be occurring without a matching Art. 13 disclosure.

Fix: Name FaceTec, IDnow, and Microblink explicitly as processors in the privacy policy, with the applicable transfer mechanism for FaceTec.

M2: Development and staging identity-verification hosts hardcoded in the production binary

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.3

A full set of development and staging hosts (ai.dev0.idnow.de through ai.dev18.idnow.de) is hardcoded alongside production hosts in the shipped APK, alongside 13 exported components and MEDIA_PROJECTION screen-capture capability noted as additional attack surface.

No reply of any kind addressed this finding.

Impact: Production release configuration hygiene falls short of separating development infrastructure from what ships to end users.

Fix: Strip development and staging endpoint configuration from production release builds.

Twelve Notices, One Automated Receipt

The only inbound message this case ever produced, across both the primary BAWAG thread and its related PayLife SESAM case, was a single fully automated acknowledgment received on 25 June 2026, the day R1 was sent, which itself instructed RFI-IRFOS not to reply to it. No DPO name was ever supplied despite R1 explicitly requesting one. No bug-bounty redirect, no customer-support misroute, and no regulator reply arrived either. Twelve notices over seventy-nine days produced silence.

A Related, Separately-Timed Case: PayLife SESAM

R1's own technical evidence, an internal storage key named BAWAG_PSK_FINGERPRINT_SHARED_PREFS and a shared application class, establishes that PayLife SESAM (at.paylife.sesam) runs on the same underlying BAWAG P.S.K. banking codebase under a different brand and icon. That case was opened separately on 6 July 2026 under REF AT-PAYLIFE-2026-R1 and carries its own embargo of 4 October 2026, not yet due. It covers its own additional findings, including an unverified certificate-pinning configuration and pre-consent Firebase/ML Kit initialization, and will be reported on its own embargo date rather than folded into this one.

Data Protection, Article by Article

Finding	Provision	Concern
H1	GDPR Art. 6(1), Art. 7	Ad-ID processing with no consent gate
H2	GDPR Art. 32	Extractable Firebase project key, unconfirmed access controls
H3	GDPR Art. 13(1)(e), Art. 44	Screenshot-capable feedback SDK on a banking app, US recipient
M1	GDPR Art. 9, Art. 13(1)(e), Art. 44	Undisclosed biometric processor and US transfer
M2	GDPR Art. 32	Development infrastructure hardcoded in production release

Disclosure Timeline & Outcome

Date	Event
2026-06-25	R1 sent to datenschutz@bawagpsk.com/datenschutz@bawag.at, 3 HIGH + 2 MEDIUM findings; automated receipt confirmation received same day
2026-07-03	Follow-up #3; Austrian DSB and EDPS added to cc
2026-07-17	Follow-up #5 restates AD_ID, Usabilla, and FaceTec findings
2026-08-31	Follow-up #10, sixty-seven days, ten messages, one automated acknowledgment
2026-09-12	Follow-up #12, seventy-nine days, twelve messages, zero reply; deadline restated as 19 September
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Name an Art. 37 Data Protection Officer and a functional escalation path beyond the datenschutz@ mailbox.
- Deploy a consent-management platform gating advertising-identifier collection.
- Confirm Firestore security rules and App Check enforcement for the exposed Firebase project.
- Disclose FaceTec, IDnow, and Microblink explicitly as processors in the privacy policy.

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. Research activity protected under Austria's Forschungsfreiheitsgesetz (Art. 17 StGG). GDPR Art. 6, 7, 9, 13, 25, 32, 44. REF BAWAG-2026-R1.