



Security & Privacy Disclosure, Final Report

PayLife SESAM Android (at.paylife.sesam)

PayLife SESAM runs on the BAWAG banking codebase, ships no pinned TLS configuration and starts Firebase before consent, and six messages over 68 days drew no reply

PUBLIC DISCLOSURE, 17 OCTOBER 2026: EMBARGO REACHED 4 OCTOBER 2026, SEVEN MESSAGES SENT, NO REPLY OF ANY KIND, THREE QUESTIONS UNANSWERED

Target	BAWAG P.S.K. Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG, Vienna (FN 269842b), operator of the PayLife brand
Package	at.paylife.sesam v3.27.2
Platform Audited	Android, root level code analysis of the production APK
Initial Disclosure (R1)	2026-07-06, to datenschutz@bawag.at, CC service@paylife.at, communications@bawaggroup.com, Austrian Datenschutzbehörde, EDPS
Disclosure / Embargo Date	2026-10-04
Report Published	2026-10-17
Overall Severity	HIGH
Findings	6 (2 High, 3 Medium, 1 Low, 0 Critical)
Correspondence	7 messages sent by RFI-IRFOS: 6 in the disclosure thread over 68 days (2026-07-06 to 2026-09-12) and 1 separate follow-up on 2026-07-28 to stop-phishing@paylife.at; 0 replies, 0 automatic acknowledgments, 0 bounces; 35 days of silence after the last message
Authorities Notified	Austrian Datenschutzbehörde · EDPS

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	5
4	Findings	5
4.1	H1: No network security configuration and no configured certificate pin on a banking app TLS channel	5
4.2	H2: Pre-consent Firebase and ML Kit auto-init, no named CMP	6
4.3	M1: Firebase/Google API key hardcoded in the production binary	6
4.4	M2: Braze, Usabilla and Countly in a banking app with US-hosted endpoints .	7
4.5	M3: Advertising and Privacy Sandbox permissions without an ad-serving SDK	7
4.6	L1: Test and debug scaffolding exported in the production release	7
5	Impact Analysis	8
6	The Complete Chain: Seven Messages, 103 Days, Zero Replies	8
7	Data Protection: Article by Article	8
8	Regulatory & Legal Landscape	9
9	Indicators of Compromise	9
10	Disclosure Timeline & Outcome	10
11	Residual Risk & Recommendations	10

Executive Summary

PayLife SESAM presents as a separate payment brand. The binary shows otherwise: the Application class is com.bawagpsk.bawagpsk.App, a SharedPreferences file is named BAWAG_PSK_FINGERPRINT_SHARED_PREFS, the PSD2 signing domain resolves to easy-bank.at, and the app talks to bawaggroup.com and bawag.at hosts. The PayLife imprint states that PayLife is a brand of BAWAG P.S.K. AG. Every finding therefore concerns BAWAG engineering practice. The BAWAG retail app disclosure (REF BAWAG-2026-R1) was published separately on 19 September 2026.

The app handles card data well: EncryptedSharedPreferences with masked card numbers, SQLCipher, comprehensive backup exclusion, biometric-bound keys and root and hook detection. Two findings carry HIGH weight. H1: no network security configuration and no configured pin value, although pinning method names such as enableCertificatePinning and setupTlsPinning exist in the code. H2: FirebaseInitProvider and MLKitInitProvider start at process creation with no consent management platform; Google Consent Mode defaults are set to deny, which limits analytics payloads and leaves Firebase Installations identifier creation untouched. Three MEDIUM findings cover a hardcoded Firebase key (withheld), Braze, Usabilla and Countly in a banking app with US endpoints, and advertising permissions without an ad SDK. One LOW finding covers androidx.test and Compose Preview activities exported in the release build.

RFI-IRFOS sent the findings on 6 July 2026 and five follow-ups in the same thread (24 July, 12 August, 24 August, 3 September, 12 September 2026) to datenschutz@bawag.at, plus one separate message to stop-phishing@paylife.at on 28 July 2026. No message drew a reply or an automatic acknowledgment. The embargo of 4 October 2026 passed 13 days before this report publishes.

ID	Severity	Title
H1	HIGH	No network security configuration and no configured certificate pin on a banking app TLS channel
H2	HIGH	Pre-consent Firebase and ML Kit auto-init, no named CMP
M1	MEDIUM	Firebase/Google API key hardcoded in the production binary
M2	MEDIUM	Braze, Usabilla and Countly in a banking app with US-hosted endpoints
M3	MEDIUM	Advertising and Privacy Sandbox permissions without an ad-serving SDK
L1	LOW	Test and debug scaffolding exported in the production release

Subject & Operator Context

PayLife publishes in its own imprint that it is a brand of BAWAG P.S.K. Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse Aktiengesellschaft, Wiedner Gürtel 11, 1100 Vienna (FN 269842b, UID ATU72252867), with the same entity named as controller in the PayLife privacy policy and datenschutz@bawag.at as the privacy contact. The Austrian Datenschutzbehörde is the competent lead authority. FMA, ECB and EBA hold banking supervision roles that do not decide GDPR competence.

Engagement Summary

RFI-IRFOS wrote to the published BAWAG privacy contact and copied the PayLife service address and the BAWAG group communications address together with the Austrian Datenschutzbehörde and the EDPS. From the follow-up of 3 September 2026 the authorities no longer appear in the CC line. Each message restated the findings and three yes/no questions on pinning, pre-consent initialisation and marketing SDKs.

Findings

H1: No network security configuration and no configured certificate pin on a banking app TLS channel

HIGH, CVSS v4.0 AV:A/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 7.6 (banking channel TLS trust)

```
AndroidManifest.xml: no android:networkSecurityConfig ; no network_security_config.xml
in the APK
classes5.dex: enableCertificatePinning, enablePublicKeyPinning, setupTlsPinning,
"[Init] Enabling certificate pinning", "Certificate pinning failure!"
grep sha256/ pin values in classes.dex..classes7.dex -> no match
```

Impact: TLS trust rests on the device system CA store alone. A party that controls a trusted root on the device (enterprise MDM profile, security software, rooted or compromised handset) can read and modify the channel between the app and its backend. The app signs PSD2 transactions and manages cards. Pinning code exists under the names enableCertificatePinning and setupTlsPinning, and no pin value is configured in the binary.

H2: Pre-consent Firebase and ML Kit auto-init, no named CMP

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.9 (pre-consent initialisation)

```
AndroidManifest.xml: FirebaseInitProvider initOrder=100 directBootAware=true ;
    MLKitInitProvider initOrder=99
    google_analytics_default_allow_analytics_storage = false (and ad_storage,
        ad_user_data, ad_personalization_signals)
    IABTCF_* constants only, no CMP vendor strings
```

Impact: Firebase and Google Measurement components initialise as ContentProviders during Application creation, mechanically before any screen or consent notice can render. Processing starts on first launch for every installation, before consent can be given. Google Consent Mode defaults are set to deny for analytics storage, ad storage, ad user data and personalisation, which narrows analytics payloads. Firebase Installations still creates a per-install identifier at first launch. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the processing starts on every installation of a banking app before any consent surface can render, and creates a persistent per-install identifier at Google.

M1: Firebase/Google API key hardcoded in the production binary

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

```
res/values/strings.xml:
    google_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately in R1]
    project_id, google_app_id: [REDACTED IN PUBLIC REPORT -- disclosed privately in R1]
```

Impact: A Firebase API key and project identifier are readable from res/values/strings.xml. No Realtime Database URL is present in this build. Google documents such keys as non-confidential; the exposure is quota abuse and reliance on server-side restrictions.

M2: Braze, Usabilla and Countly in a banking app with US-hosted endpoints

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1 (marketing SDKs)

```
sdk.iad-01.braze.com ; BANNERS_ELIGIBILITY_SHARED_PREFS,
    FEATURE_FLAGS_ELIGIBILITY_SHARED_PREFS, PUSH_DELIVERY_STORAGE_SHARED_PREFS
api.usabilla.com ; ly.count.android.sdk.messaging.CountlyPushActivity
```

Impact: Braze drives banner, feature flag and push targeting through local eligibility stores and a US region endpoint. Usabilla and Countly add feedback and push messaging. The transfer mechanism for these US vendors is not disclosed on the pages checked.

M3: Advertising and Privacy Sandbox permissions without an ad-serving SDK

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1 (permission surface)

```
AndroidManifest.xml: com.google.android.gms.permission.AD_ID,
    ACCESS_AD SERVICES_ATTRIBUTION, ACCESS_AD SERVICES_AD_ID
```

Impact: AD_ID and both Privacy Sandbox advertising permissions are declared and no ad network SDK is bundled, so the permissions most plausibly derive from Google SDK defaults and serve no banking function.

L1: Test and debug scaffolding exported in the production release

LOW, CVSS v4.0 AV:L/AC:H/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.0 (build hygiene)

```
AndroidManifest.xml: androidx.test.core.app.
    InstrumentationActivityInvoker$BootstrapActivity exported=true
    androidx.compose.ui.tooling.PreviewActivity exported=true ; <profileable android:
        shell="true"/>
```

Impact: androidx.test InstrumentationActivityInvoker activities and the Compose PreviewActivity are exported in the release, and profileable shell=true allows local profiler attachment. No data leak is shown; the surface is unnecessary in a banking release.

Impact Analysis

The findings describe fixable engineering gaps in an app that otherwise handles card data carefully. The procedural record weighs heavier: a bank operator received seven messages over 103 days at its published privacy contact and acknowledged none.

The Complete Chain: Seven Messages, 103 Days, Zero Replies

Step 1: Disclosure sent on 6 July 2026 with embargo 4 October 2026.

Step 2: Follow-up on 24 July 2026. No reply.

Step 3: Separate follow-up on 28 July 2026 to stop-phishing@paylife.at with the Austrian Datenschutzbehörde in CC. No reply.

Step 4: Follow-ups on 12 August and 24 August 2026. No reply.

Step 5: Follow-ups on 3 September and 12 September 2026, 68 days after the disclosure. No reply.

Step 6: Embargo passes on 4 October 2026 with the correspondence unanswered.

Step 7: Publication on 17 October 2026, 103 days after the disclosure and 13 days after the embargo, with the full record intact: seven messages, no reply, no acknowledgment.

Data Protection: Article by Article

Art. 32(1)(a)(b) GDPR: H1, TLS trust without configured pinning in a banking app that signs PSD2 transactions.

Art. 6(1), Art. 7(1), Art. 5(1)(a) GDPR and Art. 5(3) ePrivacy: H2, pre-consent initialisation and Firebase Installations identifier.

Art. 32(1)(b), Art. 25, Art. 5(2) GDPR: M1 hardcoded key; L1 test scaffolding in release.

Art. 5(1)(c), Art. 25, Art. 44 to 49 GDPR: M2 Braze, Usabilla and Countly with US endpoints; M3 advertising permissions.

Regulatory & Legal Landscape

BAWAG P.S.K. AG is an Austrian credit institution with its main establishment in Vienna, so the Austrian Datenschutzbehörde holds lead competence. The Austrian Datenschutzbehörde and the EDPS were in CC on the first four messages.

Fine exposure under GDPR: Art. 83(4) applies to the Art. 32 issues in H1, M1 and L1, up to EUR 10,000,000 or 2% of total worldwide annual turnover. Art. 83(5) applies to the Art. 6, Art. 7 and Art. 44 issues in H2 and M2, up to EUR 20,000,000 or 4% of total worldwide annual turnover. The same operator received a parallel disclosure for its retail banking app, which RFI-IRFOS published on 19 September 2026 after an equal silence.

Indicators of Compromise

Root level code analysis of the published application. No servers, accounts or infrastructure of the operator were probed. Credentials and identifiers referenced below are withheld from this public report; full values were disclosed privately in the R1 letter.

```
H1: no network_security_config.xml, no android:networkSecurityConfig ; classes5.dex:
    enableCertificatePinning, setupTlsPinning,
"[Init] Enabling certificate pinning" ; no populated sha256/ pin value in classes.
dex to classes7.dex

H2: FirebaseInitProvider initOrder=100, MLKitInitProvider initOrder=99 ;
    google_analytics_default_allow_* = false

M1: res/values/strings.xml google_api_key, project_id [REDACTED IN PUBLIC REPORT --
    disclosed privately in R1]

M2: Braze sdk.iad-01.braze.com, Usabilla api.usabilla.com, Countly push

M3: AD_ID, ACCESS_ADSERVICES_ATTRIBUTION, ACCESS_ADSERVICES_AD_ID

L1: androidx.test InstrumentationActivityInvoker activities exported, android.test.
    runner, profileable shell=true
```

Disclosure Timeline & Outcome

2026-07-06 Initial disclosure sent. Embargo stated as 2026-10-04.

2026-07-24 Follow-up, 18 days. No reply.

2026-07-28 Separate follow-up to stop-phishing@paylife.at, Austrian Datenschutzbehörde in CC. No reply.

2026-08-12 Second follow-up in the thread. No reply.

2026-08-24 Third follow-up. No reply.

2026-09-03 Fourth follow-up, 59 days. No reply.

2026-09-12 Fifth follow-up, 68 days. No reply.

2026-10-04 Embargo date reached and passed with no reply.

2026-10-17 This report published, 13 days after the embargo. Correspondence record: seven RFI-IRFOS messages, zero replies, zero of three questions answered.

Residual Risk & Recommendations

H1: declare a network security configuration with a populated pin-set for services.paylife.at and the bawaggroup.com hosts, and wire the existing pinning code to it.

H2: hold Firebase and ML Kit initialisation, including Firebase Installations, until consent is recorded.

M1: restrict the Firebase key and rotate it after disclosure.

M2: document purpose, legal basis and Chapter V mechanism for Braze, Usabilla and Countly, or remove them.

M3: remove advertising permissions that no function needs.

L1: strip androidx.test activities, android.test.runner and profileable from the release variant.

Procedural: reply in writing to the three questions. RFI-IRFOS will update this report with any substantive reply.

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 root level code analysis of

the published application using publicly available tooling. No operator servers, accounts or infrastructure were probed. Credentials and database identifiers are withheld from this public report; full values were disclosed privately in the original R1 letter and remain available to the operator or to a supervisory authority on request. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF AT-PAYLIFE-2026-R1.