Coordinated Privacy Disclosure, Final Report

Lufthansa Group Shared App Platform (com.lhgroup.lhgroupapp): Lufthansa, Austrian Airlines, SWISS, Eurowings

Deutsche Lufthansa AG, Frankfurt, Germany, and its sister carriers, one shared codebase across four airlines

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, ON THE STATED EMBARGO DATE, TWENTY-TWO MESSAGES ACROSS FOUR AIRLINES, ZERO REPLY OF ANY KIND

Target	Four Lufthansa Group airline apps built on one shared application platform
Packages	com.lufthansa.android.lufthansa v9.624.3, com.austrian.connector.android v7.624.3, com.yoc.swiss.swiss v6.624.3, com.germanwings.android v26.4.0, application class com.lhgroup.lhgroupapp.AppApplication shared across all four
Operator	Deutsche Lufthansa AG (Frankfurt), Austrian Airlines AG (Vienna), Swiss International Air Lines AG (Basel), Eurowings GmbH (Cologne)
Initial Disclosure	2026-06-27
Stated Embargo	2026-09-25, as communicated directly to the target in the initial disclosure
Report Published	2026-09-25, on the stated date
Regulators	BfDI (lead SA for Lufthansa AG, Frankfurt), Austrian DSB (lead SA for Austrian Airlines, Vienna), CERT.at
Total Outbound Messages	22 across the four airlines: 7 to Lufthansa, 6 to Austrian Airlines, 8 to SWISS, 1 to Eurowings. Several original addresses bounced across all four (security@austrian.com, datenschutz@swiss.com, security@eurowings.com); accepted addresses continued receiving the full follow-up sequence.
Inbound Replies	0 across all four airlines and 22 messages. No reply, automated or human, was ever received from any LHGroup carrier.

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

1 Executive Summary 4

2 Subject & Operator Analysis 5

3 Twenty-Two Messages Across Four Airlines, Zero Reply 6

4 Findings 6

4.1 C1: Passport OCR and Session Recording Active Simultaneously in the Same Flow 6

4.2 C2: OneTrust Consent Platform Structurally Bypassed by Pre-Consent Auto-Init 7

4.3 C3: Undisclosed Cross-Brand Data Consolidation on the Shared Platform . . . 7

4.4 H1: A Second, Independent Document-Scanning SDK Alongside Microblink . . 8

4.5 H2: Identical Permission Set With No Data-Minimisation Justification 8

5 Data Protection, Article by Article 9

Executive Summary

On 27 June 2026, RFI-IRFOS disclosed to Lufthansa, Austrian Airlines, SWISS, and Eurowings, simultaneously and explicitly naming each other in every message, that all four airlines' Android apps share one application class, com.lhgroup.lhgroupapp.AppApplication, meaning a single architectural decision produces identical compliance gaps across the entire Lufthansa Group fleet, not four independent app-level failures. The most severe finding names the overlap between Microblink's BlinkID passport-OCR SDK, which reads Machine-Readable Zone data including name, nationality, date of birth, and passport number, Art. 9 GDPR special-category data by nature, and Quantum Metric's session-recording SDK, active in the same booking and check-in flow. Session recording can capture the exact form interaction where a passenger enters passport data and transmit it to US infrastructure. Neither processor is named as a data recipient in any of the four airlines' privacy policies.

A second finding names the group's own consent platform, OneTrust, present and correctly integrated at the infrastructure level, which is exactly why its bypass is notable: two ContentProviders, FirebaseInitProvider and TealiumInitProvider, both fire at app launch before OneTrust can initialize, meaning Firebase Analytics and Tealium's customer data platform begin collecting behavioral data before any consent dialog can be displayed, identically across all four apps. A hardcoded Firebase API key tied to a shared project ID (groupapp-lh-prod) confirms the shared-backend architecture directly.

A third finding is structural, not technical: the shared platform itself means a passenger who flies on multiple LHGroup carriers has behavioral data from each airline's app flowing through the same infrastructure, a cross-brand data consolidation that is not disclosed as a joint processing activity in any individual airline's privacy policy, an Art. 26 joint-controller documentation gap. Two further findings round out the disclosure: a second, independent document-scanning SDK (Scandit DataCapture, with its own dedicated pre-init ContentProvider) running alongside Microblink, meaning two separate processors both touch identity-document data with no separate Art. 13 disclosure for either; and an identical permission set across all four apps, full-device calendar read and write access, undocumented microphone recording capability, and advertising-attribution tracking, none of it justified under data minimisation in any of the four privacy policies.

Twenty-two messages were sent across the four airlines and 78 days: seven to Lufthansa, six to Austrian Airlines, eight to SWISS, and one to Eurowings (whose security@ address bounced outright and was not retried, given the shared finding was already fully documented to the other three carriers). All four carriers were cc'd or referenced in each other's disclosures throughout, and BfDI and the Austrian DSB, the respective lead supervisory authorities for Lufthansa AG and Austrian Airlines, were BCC'd on every message. Not one reply, automated or human, was ever received from any of the four airlines at any point. The 90-day embargo, stated directly to all four targets in the initial disclosure, elapses today. This report and the accompanying closure notices publish on the stated date.

Scope: Root-level static analysis of the production Android applications for Lufthansa (v9.624.3), Austrian Airlines (v7.624.3), SWISS (v6.624.3), and Eurowings (v26.4.0), all pulled from Google Play and reviewed on 27 June 2026. All four share the application class com.lhgroup.lhgroupapp.AppApplication. No account was created and no interaction with Microblink's, Quantum Metric's, OneTrust's, Tealium's, Scandit's, or Firebase's backend infrastructure was performed.

Disposition

Five findings, identical across all four airlines because they share one application binary, were disclosed on 27 June 2026, re-scored under CVSS v4.0. The overlap between Microblink's passport-OCR SDK and Quantum Metric's session-recording SDK, active simultaneously in the same booking and check-in flow, reaches HIGH/8.7 on its own computed band. OneTrust's consent platform structurally bypassed by dual pre-consent ContentProvider auto-init, and the undisclosed cross-brand data consolidation inherent to the shared platform architecture, both correct to MEDIUM. A dual document-scanning SDK stack (Microblink plus Scandit) corrects to MEDIUM. A calendar, audio, and advertising-attribution permission set with no data-minimisation justification corrects to LOW. Twenty-two messages were sent across the four airlines. Not one reply of any kind was ever received from any of them.

ID	Severity	Title
C1	HIGH	Passport OCR and Session Recording Active Simultaneously in the Same Flow
C2	MEDIUM	OneTrust Consent Platform Structurally Bypassed by Pre-Consent Auto-Init
C3	MEDIUM	Undisclosed Cross-Brand Data Consolidation on the Shared Platform
H1	MEDIUM	A Second, Independent Document-Scanning SDK Alongside Microblink
H2	LOW	Identical Permission Set With No Data-Minimisation Justification

Subject & Operator Analysis

Lufthansa, Austrian Airlines, SWISS, and Eurowings are four separate legal entities within the Lufthansa Group, sharing one application platform. BfDI is the lead supervisory authority for Deutsche Lufthansa AG (Frankfurt); the Austrian DSB is the lead supervisory authority for Austrian Airlines AG (Vienna). This is not four individual compliance failures, it is one architectural decision, pre-consent ContentProvider auto-init, passport OCR via Microblink, session recording via Quantum Metric, and OneTrust consent management structurally bypassed before it can activate, replicated across the entire LHGroup fleet.

Twenty-Two Messages Across Four Airlines, Zero Reply

Seven messages were sent to Lufthansa, six to Austrian Airlines, eight to SWISS, and one to Eurowings (whose security@ address bounced outright and was not retried, since the identical finding was already fully documented to the other three carriers in the same disclosure round). Several original addresses across the group bounced (security@austrian.com, datenschutz@swiss.com, security@eurowings.com); accepted addresses continued receiving the full follow-up sequence. BfDI and the Austrian DSB were BCC'd throughout. Not one reply, automated or human, was ever received from any of the four airlines at any point across 22 messages and 78 days.

Findings

C1: Passport OCR and Session Recording Active Simultaneously in the Same Flow

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7.

com.microblink.blinkid reads passport Machine-Readable Zone data (name, nationality, date of birth, passport number, expiry), Art. 9 GDPR special-category data by nature. com.quantummetric.instrument records user sessions including form interactions and screen content, active in the same booking and check-in flow. The overlap is the violation: session recording can capture the exact interaction where a passenger enters passport data and transmit it to Quantum Metric's US infrastructure. Neither processor is named as a data recipient in any of the four airlines' privacy policies.

```
com.microblink.blinkid (passport MRZ OCR: name, nationality, DOB, passport number)
com.quantummetric.instrument (session recording, active in same flow)
```

Impact: A passenger entering passport data across any of the four LHGroup apps has that exact interaction potentially captured by session-recording software and transmitted to US infrastructure, with neither processor disclosed anywhere in the applicable privacy policy.

Fix: Mask or exclude passport-entry screens from Quantum Metric session capture across all four apps, and name both processors in each airline's privacy policy. No confirmation that this has occurred was ever received.

C2: OneTrust Consent Platform Structurally Bypassed by Pre-Consent Auto-Init

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.

OneTrust (com.onetrust.otpublishers) is present, confirming the team knows consent is required. Two ContentProviders, FirebaseInitProvider (initOrder=100, directBootAware=true) and TealiumInitProvider (initOrder=100, timeout=10s), both fire at app launch before OneTrust can initialize, identically across all four apps. A hardcoded Firebase API key ties to a single shared project (groupapp-lh-prod), confirming the shared-backend architecture directly.

```
FirebaseInitProvider: initOrder=100, directBootAware=true
TealiumInitProvider: initOrder=100, timeout=10s
google_api_key: AIzaSyBB10hYV3fiAqfWo8lIrm4ebYuIt3FCsT8, project_id: groupapp-lh-prod
```

Impact: Firebase Analytics and Tealium's customer data platform begin collecting behavioral data before any consent dialog can be displayed, on every LHGroup app, a platform-level architectural decision, not four independent implementation errors.

Fix: Gate both ContentProviders' initialization behind OneTrust's own consent status across the shared platform. No confirmation that this has occurred was ever received.

C3: Undisclosed Cross-Brand Data Consolidation on the Shared 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.

The application class com.lhgroup.lhgroupapp.AppApplication is a shared framework serving all four LHGroup airlines. A passenger who travels on multiple LHGroup carriers has behavioral data from each brand's app flowing through the same platform infrastructure. This cross-brand data consolidation is not disclosed as a processing activity in any of the four individual airline privacy policies.

Impact: The relationship between Lufthansa and its sister airlines as joint data controllers for platform-level data requires documentation under Art. 26, which is absent from every one of the four applicable privacy policies reviewed.

Fix: Document the joint-controller relationship under Art. 26 and disclose cross-brand data flows in each airline's privacy policy. No confirmation that this has occurred was ever received.

H1: A Second, Independent Document-Scanning SDK Alongside Microblink

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.

Scandit DataCapture ships with a dedicated IdLibraryLoaderContentProvider (initOrder=10), indicating the ID/document scanning module is actively configured, independently of Microblink BlinkID named in C1. The app therefore runs two separate document-scanning processors touching identity-document data.

```
Scandit DataCapture: IdLibraryLoaderContentProvider, initOrder=10 (active, alongside
    Microblink BlinkID)
```

Impact: Two independent processors both process identity-document data, each requiring its own Art. 13 disclosure and Art. 28 data processing agreement, neither of which was located in any of the four privacy policies.

Fix: Document both document-scanning SDKs separately in the privacy policy, with a stated purpose for running two in parallel. No confirmation that this has occurred was ever received.

H2: Identical Permission Set With No Data-Minimisation Justification

LOW, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 2.4.

READ_CALENDAR, WRITE_CALENDAR, RECORD_AUDIO, and ACCESS_ADSERVICES_ATTRIBUTION plus AD_ID are all declared identically across all four apps: full-device calendar read access, undocumented audio recording capability, and advertising-attribution tracking on a flight-booking app.

Impact: None of these permissions are documented with a data-minimisation justification in any of the four privacy policies, a shared gap that follows directly from the shared codebase.

Fix: Document a specific purpose for each permission across all four apps, or remove those without one. No confirmation that this has occurred was ever received.

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. 9, Art. 13(1)(e), Art. 32	C1	Passport OCR and session recording active simultaneously, both undisclosed.
Art. 6, Art. 7	C2	Consent platform structurally bypassed by pre-consent SDK initialization.
Art. 13, Art. 26	C3	Undisclosed cross-brand data consolidation, no joint-controller documentation.
Art. 13, Art. 28	H1	Second document-scanning SDK, no separate disclosure.
Art. 5(1)(c)	H2	Identical permission set with no data-minimisation justification.

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. In this report, C1 corrects to HIGH on its own computed band. C2, C3, and H1 correct to MEDIUM, and H2 corrects to LOW, all on their own computed bands. These findings and scores apply identically to all four LHGroup apps named above, since they share one application binary. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: LHGROUP-2026-PLATFORM.