Coordinated Privacy Disclosure, Final Report

Aidu.de Android (de.unister.aidu)

Operated by Invia.de (successor entity), Leipzig, Germany

ACK, THEN SILENT ON SUBSTANCE · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, ON THE STATED EMBARGO DATE

Target	Aidu.de, a German travel-deals platform
Package	de.unister.aidu, version 2.23.2
Operator	Invia.de, Leipzig, Germany, the verified successor entity operating the Aidu.de brand
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	Germany's BfDI, Austrian DSB, CERT.at
Total Outbound Messages	5, across 71 days; the original addresses at aidu.de bounced on DNS failure, correspondence continued with Invia's legal contact once identity was verified.
Inbound Replies	One identity-verification question from Invia's Mirko Richter (cc: recht@invia.de), confirmed genuine on 2026-07-20. No substantive reply to the three open questions or the two CRITICAL findings was ever received. One out-of-office auto-reply, 2026-09-06.

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

Contents

Executive Summary

On 27 June 2026, RFI-IRFOS disclosed to Aidu.de, a German travel-deals platform, that its Android app initialises UXCam, a screen-recording and screenshot SDK, via UXCamContentProvider at process attach, meaning app screenshots are captured and transmitted to UXCam's US infrastructure before the app's own Usercentrics consent dialog has been shown to the user. This computes to MEDIUM/6.9 under CVSS v4.0.

A second finding: the app's Firebase backend project is named ab-in-den-urlaub-flutter-prod, a different brand, product, and apparent controller identity than the one users believe they are interacting with when they use Aidu.de. This raises a direct question under GDPR Art. 13(1)(a) and Art. 26 about whether users are told which legal entity actually processes their data, and whether a joint-controller arrangement with Ab-in-den-Urlaub.de exists and is documented. This also computes to MEDIUM/6.9.

A third finding: Exponea/Bloomreach, a full customer-data platform running 1,016 compiled classes across behavioral analytics, campaign automation, and push messaging, the largest SDK in the app, is not named as a data processor under Art. 13(1)(e). This computes to MEDIUM/6.9 as well.

The original disclosure addresses at aidu.de all hard-bounced on DNS failure, the domain itself does not resolve for mail. Once RFI-IRFOS identified Invia.de as the verified successor entity actually operating the Aidu.de brand and redirected correspondence to Mirko Richter with Invia's legal team (recht@invia.de) in copy, one genuine reply was received on 2026-07-20: a request to verify that the original disclosure had genuinely come from RFI-IRFOS. That verification was confirmed the same day, along with a full restatement of the two most serious findings and the three specific open questions. Four further follow-ups (2026-08-15, 2026-08-24, 2026-09-06, plus an out-of-office auto-reply confirming Richter's return date of 2026-09-13) produced no substantive answer to any of the three questions or either CRITICAL-labelled finding. The 90-day embargo, stated directly to the target in the initial disclosure, elapses today, twelve days after Richter's confirmed return from leave. This report and the accompanying closure notice publish on the stated date.

Scope: Root-level static analysis of the production Aidu.de Android application (de.unister.aidu, version 2.23.2), pulled from Google Play and reviewed on 27 June 2026. No account was created and no interaction with UXCam's, Exponea/Bloomreach's, or Firebase's backend infrastructure was performed.

Disposition

Three findings were disclosed on 27 June 2026, re-scored under CVSS v4.0. UXCam capturing app screenshots before the Usercentrics consent dialog appears, a Firebase backend project belonging to a different brand identity (ab-in-den-urlaub-flutter-prod) than the one users believe they are interacting with, and an undisclosed 1,016-class Exponea/Bloomreach customer-data platform, all correct to MEDIUM. The original aidu.de addresses hard-bounced on DNS failure; once redirected to Invia's legal contact, one identity-verification exchange occurred, followed by silence on all three substantive questions across four further follow-ups.

ID	Severity	Title
C1	MEDIUM	UXCam Captures Screenshots Before the App's Own Consent Dialog Appears
C2	MEDIUM	Firebase Backend Project Belongs to a Different Brand Identity
H1	MEDIUM	Undisclosed Customer-Data Platform, 1,016 Classes

Subject & Operator Analysis

The domain aidu.de itself does not resolve for mail, all three original disclosure addresses hard-bounced on DNS failure. RFI-IRFOS identified Invia.de, Leipzig, Germany, as the verified successor entity actually operating the Aidu.de brand, and redirected correspondence accordingly.

One Verification Exchange, Then Silence on Substance

Invia's Mirko Richter, with the company's legal team (recht@invia.de) in copy, wrote once to verify that the original disclosure had genuinely come from RFI-IRFOS. That was confirmed the same day, 2026-07-20, along with a full restatement of both CRITICAL-labelled findings and three specific open questions addressed directly to Invia's data protection officer. Four further messages, 2026-08-15, 2026-08-24, and 2026-09-06, plus an out-of-office auto-reply confirming Richter's return date of 2026-09-13, produced no answer to any of the three questions or either finding. The embargo elapses today, twelve days after that confirmed return.

Findings

C1: UXCam Captures Screenshots Before the App's Own Consent Dialog Appears

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.

UXCam (including uxcam/screenshot) initialises via UXCamContentProvider at process attach, before the app's own Usercentrics consent dialog is shown. Screenshots of the app are transmitted to UXCam's US infrastructure before any consent signal exists.

Impact: App-screen screenshots, which can incidentally contain personal data entered by the user, are collected and transmitted before the app's own declared consent mechanism has had any opportunity to run.

Fix: Gate UXCam initialization behind the Usercentrics consent flow it is meant to sit downstream of. No confirmation that this has occurred was ever received.

C2: Firebase Backend Project Belongs to a Different Brand Identity

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 Firebase backend project is named ab-in-den-urlaub-flutter-prod, a different brand, product, and apparent controller identity than the one users believe they are interacting with when using Aidu.de.

```
firebase_project_id: ab-in-den-urlaub-flutter-prod
```

Impact: Users are not told which legal entity actually processes their data on shared infrastructure, and no joint-controller documentation under Art. 26 was found addressing this shared processing arrangement.

Fix: Disclose the actual controller identity and processing infrastructure relationship in the privacy policy, and document the joint-controller basis if Invia's brands share this backend. No confirmation that this has occurred was ever received.

H1: Undisclosed Customer-Data Platform, 1,016 Classes

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.

Exponea/Bloomreach, a full customer-data platform with behavioral analytics, campaign automation, and push messaging, runs 1,016 compiled classes, the largest SDK in the app, and is not named as a data processor.

Impact: Behavioral profiling and campaign-automation data reaches a customer-data platform with no Art. 13(1)(e) disclosure naming it as a recipient.

Fix: Name Exponea/Bloomreach as a data processor in the privacy policy and document the applicable legal basis. 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. 6, Art. 7, Art. 44	C1	UXCam captures screenshots before the app's own consent dialog appears.
Art. 13(1)(a), Art. 26	C2	Firebase backend project belongs to a different brand identity than the one users believe they interact with.
Art. 13, Art. 44	H1	Undisclosed 1,016-class customer-data platform.

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, all three findings correct to MEDIUM on their own computed bands; the original R1 correspondence labelled the first two CRITICAL by real-world impact at a time before CVSS v4.0 was adopted into the methodology, a labelling this report does not retrofit. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: AIDU-2026-R1.