



Coordinated Privacy Disclosure, Final Report

Good Calendar Android
(calendar.agenda.calendarplanner.agendaplanner)

BetterAppTech, Netherlands/Belgium

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, SIX DAYS AFTER THE EMBARGO, ELEVEN MESSAGES, FOUR BOUNCED ADDRESSES, ZERO REPLY OF ANY KIND

Target	Good Calendar, a calendar and agenda-planning Android app
Package	calendar.agenda.calendarplanner.agendaplanner
Operator	BetterAppTech, a Dutch/Belgian developer
Initial Disclosure	2026-06-25
Original Embargo	2026-09-19 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-25, six days after the embargo, an internal publishing gap, not a change in terms
Regulators	Dutch Autoriteit Persoonsgegevens (AP, lead SA), Austrian DSB, CERT.at, EDPS
Total Outbound Messages	13, across 79 days: initial attempts to contact@betterapptech.com and info@betterapptech.com bounced; calendar@betterapptech.com and support@betterapptech.com accepted the remaining messages.
Inbound Replies	0. No reply, automated or human, was ever received on any address.

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	Eleven Messages, Four Bounces, Zero Reply	5
4	Findings	6
4.1	C1: AdMob and Firebase Both Initialize Before Any Consent Screen, in an App With Calendar and Contacts Access	6
4.2	H1: All Four Privacy Sandbox Permissions and a Four-Network Ad Stack on an App With Calendar and Contacts Access	6
4.3	H2: Firebase, AdMob, and S3 Credentials Hardcoded and Extractable	7
4.4	H3: Undocumented RECORD_AUDIO Permission	7
4.5	M1: Overlay and Background-Process-Management Permissions With No Documented Purpose	8
5	Data Protection, Article by Article	8

Executive Summary

On 25 June 2026, RFI-IRFOS disclosed to BetterAppTech that its Good Calendar Android app, which holds `READ_CALENDAR`, `WRITE_CALENDAR`, `READ_CONTACTS`, and `WRITE_CONTACTS`, among the most personally sensitive data categories on a device, initializes both AdMob (`initOrder=100`) and Firebase (`initOrder=100`, `directBootAware`) as ContentProviders at process creation, before any Activity and before any consent screen. A consent dialog shown afterward cannot retroactively gate data collection that has already begun.

A second finding names the app's combined advertising footprint, not a single tracking flow: a four-network ad stack (AdMob, AppLovin, Smaato, Facebook Audience Network) runs alongside all four Privacy Sandbox permissions, including `ACCESS_AD SERVICES_CUSTOM_AUDIENCE`, which lets the app group users into behavioral cohorts, in this case built from scheduling patterns, when a user is at work, at a medical appointment, or on holiday, for targeting inside other, unrelated apps. Users granting calendar and contacts access to manage their schedule have no reason to expect that scheduling behavior itself becomes advertising-targeting material.

Eleven messages were sent across 79 days. The first attempts, to `calendar@betterapptech.com` and `privacy@betterapptech.com`, both bounced; a second attempt to `info@betterapptech.com` and `contact@betterapptech.com` also bounced; `calendar@betterapptech.com` and `support@betterapptech.com` finally accepted delivery for the remaining messages, cc'ing the Dutch AP, the Austrian DSB, CERT.at, and the EDPS on later rounds. Not one reply, automated or human, was ever received on any address at any point. The 90-day embargo, stated directly to the target in the 12 September message, elapsed on 19 September 2026. This report and the accompanying closure notice publish six days later, an internal gap on RFI-IRFOS's side, not a change to the terms already disclosed.

Scope: Root-level static analysis of the production Good Calendar Android application (`calendar.agenda.calendarplanner.agendaplanner`, version 2.07.17.0617, 87.3 MB), as pulled via ADB from a physical device and reviewed on 25 June 2026. No dynamic instrumentation, live traffic capture, or interaction with BetterAppTech's, Google's, or Meta's backend infrastructure was performed.

Disposition

Five findings were disclosed on 25 June 2026, re-scored under CVSS v4.0. All five correct to MEDIUM or LOW on their computed bands. Pre-consent AdMob and Firebase initialization in an app with calendar and contacts access, all four Privacy Sandbox permissions including Custom Audience cohort targeting, and hardcoded Firebase and AdMob credentials all correct to MEDIUM. An undocumented `RECORD_AUDIO` permission and an `overlay/process-management` permission set both correct to LOW. Eleven messages were sent across 79 days, four addresses bouncing before a working channel was found. Not one reply of any kind was ever received.

ID	Severity	Title
C1	MEDIUM	AdMob and Firebase Both Initialize Before Any Consent Screen, in an App With Calendar and Contacts Access
H1	MEDIUM	All Four Privacy Sandbox Permissions and a Four-Network Ad Stack on an App With Calendar and Contacts Access
H2	MEDIUM	Firebase, AdMob, and S3 Credentials Hardcoded and Extractable
H3	LOW	Undocumented RECORD_AUDIO Permission
M1	LOW	Overlay and Background-Process-Management Permissions With No Documented Purpose

Subject & Operator Analysis

Good Calendar is a calendar and agenda-planning app operated by BetterAppTech, a Dutch/Belgian developer, placing the Dutch Autoriteit Persoonsgegevens as lead supervisory authority.

Several genuine positives are worth naming. allowBackup is correctly set to false. A network security configuration is present. The NFC permission is justified by a confirmed Microsoft 365/Exchange enterprise authentication feature. DISABLE_KEYGUARD is justified by standard alarm/reminder wake-screen behavior, and FOREGROUND_SERVICE_DATA_SYNC is justified by calendar background sync. The app is built on a modern Jetpack Compose and Kotlin architecture.

Eleven Messages, Four Bounces, Zero Reply

This case's correspondence record involved four address failures before a working channel was found. The first attempts, to kalender@betterapptech.com and privacy@betterapptech.com, both bounced. A second attempt, to info@betterapptech.com and contact@betterapptech.com, also bounced. kalender@betterapptech.com and support@betterapptech.com finally accepted delivery for the remaining messages across the following 79 days, cc'ing the Dutch AP, the Austrian DSB, CERT.at, and, on later rounds, the EDPS. Not one reply, automated or human, was ever received on any address at any point.

Findings

C1: AdMob and Firebase Both Initialize Before Any Consent Screen, in an App With Calendar and Contacts Access

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.

Both mobileadsinitprovider (AdMob, initOrder=100) and FirebaseInitProvider (initOrder=100, directBootAware="true") are declared, both firing at process creation, before any Activity and therefore before any consent dialog. A consent screen shown afterward cannot retroactively gate the ad and analytics infrastructure that has already initialized, in an app that also holds calendar and contacts access.

```
calendar.agenda.calendarplanner.agendaplanner.mobileadsinitprovider    initOrder=100
com.google.firebase.provider.FirebaseInitProvider    initOrder=100, directBootAware=
    true
```

Impact: Advertising and analytics infrastructure is active while the app's own access to calendar events and contact data is already available, before any consent mechanism could run.

Fix: Defer both providers' initialization until after an app-native consent flow has run. No confirmation that this has occurred was ever received.

H1: All Four Privacy Sandbox Permissions and a Four-Network Ad Stack on an App With Calendar and Contacts Access

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.

AD_ID, ACCESS_ADSERVICES_ATTRIBUTION, ACCESS_ADSERVICES_TOPICS, and ACCESS_ADSERVICES_CUSTOM_AUDIENCE are all declared, alongside a four-network ad stack: AdMob, AppLovin MAX, Smaato, and Facebook Audience Network. Custom Audience enables the app to build behavioral cohorts from scheduling patterns for targeting inside other, unrelated apps.

```
AD_ID, ACCESS_ADSERVICES_ATTRIBUTION, ACCESS_ADSERVICES_TOPICS,
ACCESS_ADSERVICES_CUSTOM_AUDIENCE
AdMob, AppLovin MAX, Smaato SDK, Facebook Audience Network
AdMob app ID: ca-app-pub-4902626407763154
```

Impact: A user's scheduling behavior, when they are at work, at medical appointments, or on holiday, can be turned into a cross-app advertising targeting cohort, with no disclosed purpose located for this specific use.

Fix: Document an individual Art. 6(1) legal basis for Custom Audience targeting or remove the permission. No confirmation that this has occurred was ever received.

H2: Firebase, AdMob, and S3 Credentials Hardcoded and Extractable

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

A Firebase API key and the AdMob App ID are both hardcoded and extractable from the production binary, alongside a reference to an AWS S3 bucket in the EU-West region used for calendar sync data.

```

Firebase API key: AIzaSyC5CIGCnH7SmNVWb6xegS4rh4h7xTyIBMw
AdMob App ID: ca-app-pub-4902626407763154
S3 bucket: goodcalendarbucket.s3.eu-west-1.amazonaws.com

```

Impact: Both keys are trivially extractable; depending on the security-rule and bucket-policy configuration behind them, this could enable unauthorized access to calendar sync data or denial of service against legitimate users.

Fix: Restrict the Firebase API key by package name and SHA-1 certificate fingerprint, and audit the S3 bucket policy for public accessibility. No confirmation that this has occurred was ever received.

H3: Undocumented RECORD_AUDIO Permission

LOW, CVSS v4.0 AV:P/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 1.0.

RECORD_AUDIO is declared with no documented feature located in the app's install-time permission rationale. Voice-to-text event creation is a plausible legitimate use, but it is not disclosed.

Impact: Microphone access is present in a calendar app with no corresponding disclosed feature; the practical exploitation path requires local conditions the static review could not establish, which keeps the computed score low.

Fix: Document the specific voice feature RECORD_AUDIO supports, or remove it. No confirmation that this has occurred was ever received.

M1: Overlay and Background-Process-Management Permissions With No Documented Purpose

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.

SYSTEM_ALERT_WINDOW, allowing the app to draw over every other app on the device, and KILL_BACKGROUND_PROCESSES, allowing it to terminate other running apps, are both declared with no documented purpose in a calendar context.

Impact: Combined with the active advertising SDK stack, SYSTEM_ALERT_WINDOW is a plausible vector for overlay-ad display; the practical exploitation path requires conditions the static review could not establish, which keeps the computed score low.

Fix: Remove both permissions unless a specific, disclosed feature requires them. 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. 7, Art. 25, Art. 5(1)(b)	C1	Pre-consent ad and analytics SDK initialization in an app with calendar and contacts access.
Art. 5(1)(b), Art. 6(1), Art. 13(1)(c)	H1	Undisclosed cross-app advertising cohort targeting built from scheduling behavior.
Art. 32	H2	Hardcoded Firebase, Ad-Mob, and S3 credentials.
Art. 5(1)(b), Art. 13(1)(c)	H3	Undocumented microphone access.
Art. 5(1)(c), Art. 13(1)(c)	M1	Undocumented overlay and background-process-management permissions.

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, H1, and H2 correct to MEDIUM to match their own computed bands; H3 and M1 correct to LOW on their own computed bands. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: GOODCALENDAR-2026-R1.