Coordinated Privacy Disclosure, Final Report

Too Good To Go Android (com.app.tgtg)

Too Good To Go International A/S, Denmark, food-waste marketplace

CS-DEFLECT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, ONE DAY AFTER THE STATED 24 SEPTEMBER EMBARGO, SEVEN MESSAGES, SIX IDENTICAL AUTO-REPLIES, ZERO SUBSTANTIVE REPLY

Target	Too Good To Go, a food-waste-reduction marketplace app
Package	com.app.tgtg, version 26.6.10, versionCode 21128
Operator	Too Good To Go International A/S, Denmark
Initial Disclosure	2026-06-24
Stated Embargo	2026-09-24, as communicated directly to the target in the initial disclosure
Report Published	2026-09-25, one day after the stated date
Regulators	Danish Datatilsynet (lead SA), Austrian DSB, Germany's BfDI, CERT.at
Total Outbound Messages	7, across 62 days, to privacy@toogoodtogo.com and dpo@toogoodtogo.com.
Inbound Replies	6 identical automated template responses from privacy+canned.response@toogoodtogo.com, one following each outbound message. No substantive human reply was ever received.

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

Contents

Executive Summary

On 24 June 2026, RFI-IRFOS disclosed to Too Good To Go that three ContentProviders, Salesforce Marketing Cloud, Firebase, and Facebook, all initialize during the app's startup sequence, before Application.onCreate() executes and before any UI, including the app's own consent dialog, is rendered. Too Good To Go does ship a functional consent interface with separate toggles for necessary and optional tracking, which confirms the team understands prior consent is required, but the technical implementation starts the tracking stack before that dialog is ever shown, making the consent UI legally ineffective for these three SDKs. Firebase's directBootAware=true setting means it additionally initializes on device reboot before the device is even unlocked.

Two further findings name the specific platforms behind the pre-consent stack. Salesforce Marketing Cloud ships a dedicated LocationReceiver alongside ACCESS_FINE_LOCATION, meaning precise geographic data, purchase frequency, movement patterns, and push engagement all route to Salesforce's US infrastructure with no Art. 46 transfer mechanism visible from the app's own consent sequencing. Braze ships 46 compiled packages and a JavaScript bridge (brazeBridge.logPurchase, logCustomEvent, requestPushPermission) that tracks individual purchase events with price and quantity and can solicit push permission from within HTML in-app messages, also routing to US infrastructure.

Two further findings round out the disclosure: a Facebook client token hardcoded in plaintext in the production APK, extractable by anyone who downloads it; and READ_CALENDAR plus WRITE_CALENDAR permissions with no documented, proportionate purpose for a food-waste marketplace, revealing when a user is at work, on holiday, or at appointments. Genuine positives are worth naming: the app's network security configuration correctly scopes cleartext exceptions to debug builds only, and it supports in-app personal data export requests.

Seven messages were sent across 62 days, to privacy@toogoodtogo.com and dpo@toogoodtogo.com, cc'ing the Danish Datatilsynet (lead supervisory authority for Too Good To Go's Danish establishment), the Austrian DSB, Germany's BfDI, and CERT.at throughout. Every single message, all seven, drew an identical automated response from privacy+canned.response@toogoodtogo.com, the same template each time, which RFI-IRFOS named explicitly in a dedicated escalation as Pattern 1, Policy-as-Implementation-Proof: directing a technical disclosure to a general privacy-policy reference instead of engaging with any specific finding. Not one substantive human reply was ever received. The 90-day embargo, stated directly to the target in the initial disclosure, elapsed on 24 September 2026. This report and the accompanying closure notice publish one day 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 Too Good To Go Android application (com.app.tgtg, version 26.6.10, versionCode 21128), pulled from Google Play and reviewed on 24 June 2026. No account was created and no interaction with Salesforce's, Braze's, Firebase's, or Meta's backend infrastructure was performed.

Disposition

Five findings were disclosed on 24 June 2026, re-scored under CVSS v4.0. All five correct to MEDIUM or LOW on their own computed bands. Pre-consent initialization of three tracking SDKs (Salesforce Marketing Cloud, Firebase, Facebook), Salesforce's location receiver and behavioral profiling, Braze's purchase-tracking and in-app-messaging bridge, and a hardcoded Facebook client token all correct to MEDIUM. Undocumented calendar read and write access corrects to LOW. Seven messages were sent across 62 days. Every single one drew an identical automated canned-response template, named explicitly in the escalation as Pattern 1 (Policy-as-Implementation-Proof), and not one substantive human reply was ever received.

ID	Severity	Title
C1	MEDIUM	Three Tracking SDKs Auto-Initialize Before the App's Own Consent Dialog
C2	MEDIUM	Salesforce Location Receiver and Behavioral Profiling to US Infrastructure
C3	MEDIUM	Braze Purchase-Tracking and In-App-Messaging Bridge to US Infrastructure
H1	MEDIUM	Hardcoded Facebook Client Token in the Production APK
H2	LOW	Undocumented Calendar Read and Write Access

Subject & Operator Analysis

Too Good To Go International A/S is established in Denmark, placing the Danish Datatilsynet as lead supervisory authority under Art. 55-56 GDPR.

Genuine positives are worth naming. Too Good To Go's network security configuration correctly scopes cleartext exceptions to debug builds only, meaning production traffic is not subject to user-installed certificate overrides. The app supports in-app personal data export requests. The functional consent interface with separate toggles for necessary and optional tracking shows real effort at the design level, the gap named in this report is specifically that the underlying SDK initialization does not honor that interface.

Seven Messages, Six Identical Auto-Replies, Zero Substantive Reply, Named as Pattern 1

Every one of the seven messages in this case's correspondence record drew an identical automated response from privacy+canned.response@toogoodtogo.com, the same template each time, directing the recipient to review the general privacy policy instead of engaging with any of the five specific technical findings. RFI-IRFOS named this explicitly in a dedicated escalation on 28 June 2026 as Pattern 1, Policy-as-Implementation-Proof, a response pattern that treats the existence of a published policy as proof that its own binary complies with it. Not one substantive human reply was ever received across the full 62-day record.

Findings

C1: Three Tracking SDKs Auto-Initialize Before the App's Own Consent Dialog

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.

Salesforce Marketing Cloud, Firebase, and Facebook each register a ContentProvider that Android auto-initializes at process start, before Application.onCreate() runs and before any UI, including the app's own consent dialog, is rendered. Firebase's provider is additionally directBootAware="true", meaning it initializes on device reboot before the device is even unlocked.

```
com.salesforce.marketingcloud.MCInitContentProvider
com.google.firebase.provider.FirebaseInitProvider: directBootAware=true, initOrder=100
com.facebook.internal.FacebookInitProvider
```

Impact: Too Good To Go's own consent dialog exists and offers a genuine choice, but three tracking SDKs are already running by the time it renders, making that choice legally ineffective for the data those three SDKs collect before the user ever sees the screen.

Fix: Gate all three ContentProviders' initialization behind the existing consent flow. No confirmation that this has occurred was ever received.

C2: Salesforce Location Receiver and Behavioral Profiling to US Infrastructure

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.

Salesforce Marketing Cloud ships a dedicated com.salesforce.marketingcloud.location.LocationReceiver, combined with ACCESS_FINE_LOCATION. Purchase frequency, geographic movement patterns, push notification engagement, and browsing behavior all route to Salesforce, Inc. (San Francisco), a US company, with no Art. 46 transfer mechanism visible given the pre-consent initialization in C1.

```
com.salesforce.marketingcloud.location.LocationReceiver
ACCESS_FINE_LOCATION declared
```

Impact: Precise location and behavioral-purchase data reach a US marketing automation platform through infrastructure that initializes before any consent basis exists for the transfer.

Fix: Document the Art. 46 transfer mechanism covering Salesforce, and ensure location data collection is itself gated behind consent. No confirmation that this has occurred was ever received.

C3: Braze Purchase-Tracking and In-App-Messaging Bridge to US Infrastructure

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.

46 compiled packages under com/braze/ and com/appboy/ ship alongside a JavaScript bridge (assets/braze-html-bridge.js) exposing logPurchase(productId, price, currencyCode, quantity), logCustomEvent(name, properties), and requestPushPermission(). This is a full lifecycle marketing platform, not passive analytics, tracking individual purchase events with price and quantity and able to solicit push permission from within HTML in-app messages. Braze, Inc. is a US company (New York).

```
brazeBridge.logPurchase(productId, price, currencyCode, quantity, purchaseProperties)
brazeBridge.logCustomEvent(name, properties)
brazeBridge.requestPushPermission()
```

Impact: Individual purchase events, with price and quantity, are tracked and transmitted to US infrastructure through a bridge that initializes before consent, the same underlying issue as C1 and C2.

Fix: Document the Art. 46 transfer mechanism covering Braze, and gate the bridge's initialization behind consent. No confirmation that this has occurred was ever received.

H1: Hardcoded Facebook Client Token in the Production APK

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.

A Facebook client token and app ID are hardcoded in plaintext in res/values/strings.xml , extractable by anyone who downloads the APK.

```
fb_token: 6aee551064c356226f35160a52309f6a
fb_id: 184721518527049
```

Impact: Any party with the APK can use the extracted token to make authenticated requests against Too Good To Go's own Facebook application.

Fix: Rotate the token and restrict it server-side. No confirmation that this has occurred was ever received.

H2: Undocumented Calendar Read and Write Access

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.

Both READ_CALENDAR and WRITE_CALENDAR are declared, with no identifiable proportionate purpose for a food-waste marketplace. Calendar data reveals when a user is at work, on holiday, at appointments, or at home.

Impact: Full-calendar read access on a food-marketplace app exceeds what its documented function requires, with no disclosed feature justifying it.

Fix: Remove READ_CALENDAR unless a specific, disclosed feature requires it. No confirmation that this has occurred was ever received.

Article	Finding	Basis

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. 5(1)(a), ePrivacy Art. 5(3)	C1	Pre-consent initialization of three tracking SDKs.
Art. 6(1), Art. 44-46, Art. 13(1)(f)	C2	Salesforce location receiver and behavioral profiling to US infrastructure.
Art. 6(1), Art. 44-46	C3	Braze purchase-tracking and in-app-messaging bridge to US infrastructure.
Art. 5(1)(f), Art. 32	H1	Hardcoded Facebook client token.
Art. 5(1)(c), Art. 13	H2	Undocumented calendar read and write access.

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, C2, C3, and H1 correct to MEDIUM on their own computed bands. H2 corrects to LOW. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF #TGTG-001.