



Coordinated Security & Privacy Disclosure, Final Report

Temu for Android (com.einnovation temu)

A shopping app whose own code names itself Baogong, PDD Holdings' internal Pinduoduo engineering stack, ninety days of total silence

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY DAYS, ZERO REPLIES OF ANY KIND

Target	Whaleco Technology Limited, Dublin, Ireland (disclosed EU controller); PDD Holdings Inc., Shanghai, China (identified operator of the underlying codebase)
Product audited	Temu for Android, com.einnovation temu, v4.60.0
Disclosure reference	REF TEMU-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 controller-identity concealment, C2 undisclosed social-commerce infrastructure, CVSS v4.0 8.7)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

1	Executive Summary	3
2	Subject & Operator Analysis	4
3	Positive Observations	4
4	Findings	4
4.1	C1: Controller-identity concealment: the disclosed EU controller does not match the app's own codebase origin	4
4.2	C2: Undisclosed Pinduoduo social-commerce and chat infrastructure embedded in the EU shopping app	5
4.3	H1: minSdk 23 (Android 6.0, 2015) for a payment-processing app	5
4.4	H2: Braintree/PayPal payment SDK present as an unnamed EU payment processor	6
4.5	H3: Opaque WebView container with a server-controlled capability surface . .	6
5	Data Protection, Article by Article	6
6	Disclosure Timeline & Outcome	7
7	Residual Risk & Recommendations	8

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production Temu Android application, downloaded from the public Google Play Store, no account created, no backend access, no user data touched, and identified five findings, two CRITICAL, three HIGH. The most significant: Temu's EU consent framework names Whaleco Technology Limited (Dublin, Ireland) as the data controller, but the production APK's own smali code is organized under the namespace prefix `com/baogong/`, PDD Holdings' asserted internal engineering codename for its Pinduoduo platform, with module architecture (`app_login`, `chat`, `home`, `order_list`) matching the Pinduoduo engineering stack rather than a Whaleco-native codebase.

Separately, 626 smali classes under `com/baogong/chat/` implement a complete social-commerce and chat infrastructure, including AI chat with server-side prompt injection and cart-sharing between users, active and present in the EU consumer APK available on the Google Play Store. EU consumers using what presents as a shopping app did not separately consent to social graph construction or conversation metadata collection for this purpose.

Eight written notices were sent over 90 days. Not one produced a reply of any kind, substantive, automated, or a bounce (with one address, `press@temu.com`, itself non-existent). All five findings stand exactly as originally reported.

Scope: Static analysis of the publicly downloaded production Temu Android APK, on an authorized test device, only. No Temu/Whaleco account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 20 June 2026 to `legal@temu.com`, bcc the Irish DPC (Whaleco Technology Limited's lead supervisory authority), the Austrian DSB, CERT.at, and the EDPB. Seven further written notices followed through 4 September 2026, cc `dsb@dsb.gv.at` and `Dispute@temu.com`. No reply of any kind, human or automated, was ever received from `legal@temu.com` or `Dispute@temu.com` across the entire 90 day window.

ID	Severity	Title
C1	CRITICAL	Controller-identity concealment: the disclosed EU controller does not match the app's own codebase origin
C2	CRITICAL	Undisclosed Pinduoduo social-commerce and chat infrastructure embedded in the EU shopping app
H1	HIGH	minSdk 23 (Android 6.0, 2015) for a payment-processing app
H2	HIGH	Braintree/PayPal payment SDK present as an unnamed EU payment processor
H3	HIGH	Opaque WebView container with a server-controlled capability surface

Subject & Operator Analysis

Temu is operated for EU users under the disclosed controller Whaleco Technology Limited (Dublin, Ireland); RFI-IRFOS's finding is that the app's own codebase identifies its actual engineering origin as PDD Holdings' Pinduoduo platform, Shanghai, China.

Positive Observations

No specific positive controls were identified as a distinct section in the original disclosure; the audited binary's primary characteristics are addressed directly in the findings above.

Findings

C1: Controller-identity concealment: the disclosed EU controller does not match the app's own codebase origin

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

Temu's EU consent framework names Whaleco Technology Limited (Dublin, Ireland) as data controller; the privacy policy elsewhere names Whaleco Inc. (Boston, Massachusetts, US). The production APK's smali code is organized under com/baogong/, asserted as PDD Holdings' internal engineering codename for Pinduoduo.

```
com/baogong/app_login/  
com/baogong/chat/  
com/baogong/business/  
com/baogong/home/  
com/baogong/ui/  
com/baogong/order_list/  
com/baogong/router/  
com/baogong/base/  
com/baogong/app_baogong_shopping_cart/  
com/baogong/app_goods_detail/  
com/baogong/shop/
```

No response was received naming this finding, including the direct question of whether Whaleco Technology Limited is genuinely the Art. 4(7) GDPR controller for the com.baogong codebase, given PDD Holdings' Shanghai operations and exposure to China's National Security Law Art. 7 and Data Security Law Art. 35, which require Chinese entities to cooperate with state intelligence access requests. This corroborates an independent noyb complaint against Temu filed in January 2025.

Impact: EU users are told a Dublin/Boston entity controls their data while the underlying codebase and, by inference, its development and operational access, traces to a China-headquartered organization subject to state intelligence access obligations, with no disclosed Art. 46 transfer safeguard.

Fix: Accurately disclose the actual controller and processing entities under Art. 13(1)(a), and

publish the Art. 46 transfer mechanism covering the com.baogong codebase's origin and any associated operational access from China.

C2: Undisclosed Pinduoduo social-commerce and chat infrastructure embedded in the EU shopping app

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

626 smali classes under com/baogong/chat/ implement a complete social-commerce and messaging layer, active in the EU consumer APK available on the Google Play Store.

```
ConversationListComponentV2
ChatBottomContainer
MessageFlowComponent
SystemPromptBinder      <- AI chat with server-side prompt injection
OtterChatPushServiceImpl <- background push for social messages
ShoppingCartShareFragment <- cart-sharing with other users
OtterLauncherJob         <- background social-layer initialisation
```

No response was received naming this finding. Temu presents as a shopping app but ships the full social-commerce infrastructure of Pinduoduo, social graph exploitation, group buying, peer-to-peer product sharing. EU consumers did not consent to social graph construction, conversation metadata collection, or server-side-prompted AI chat as part of a stated shopping purpose.

Impact: A complete, active social-commerce and chat layer processes conversation and social-graph data from EU shopping-app users with no separate disclosed purpose or consent basis distinct from the app's stated shopping function.

Fix: Disclose the social-commerce and chat infrastructure as a distinct processing activity under Art. 13, and obtain separate consent for social graph construction and conversation metadata collection.

H1: minSdk 23 (Android 6.0, 2015) for a payment-processing app

MEDIUM, CVSS v4.0 AV:P/AC:H/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N, 5.4

The app declares minSdk 23. Android 6 devices have received no Google security patches in over six years.

No response was received naming this finding.

Impact: A payment-processing shopping app supports devices with no current security patches, disproportionate exposure for any user still on this baseline.

Fix: Raise minSdk to a currently-patched Android baseline.

H2: Braintree/PayPal payment SDK present as an unnamed EU payment processor

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

261 Braintree/PayPal classes handle payment processing without being named as a distinct processing party to users.

No response was received naming this finding.

Impact: Payment data is processed by an unnamed third party with no disclosed Art. 28 processor relationship.

Fix: Name Braintree/PayPal as a payment processor under Art. 13(1)(e).

H3: Opaque WebView container with a server-controlled capability surface

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

A WebView container component ("ITpwContainerAPI"), 442 classes, exposes server-controlled capabilities not auditable from the APK alone.

No response was received naming this finding.

Impact: A server-controlled capability surface within the app cannot be independently audited from the client binary, and its full scope is undisclosed.

Fix: Publish the documented capability surface exposed through this WebView container and its data-processing implications.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 13(1)(a), Art. 5(1)(a), Art. 46	Disclosed controller does not match code-base origin
C2	GDPR Art. 5(1)(b), Art. 13	Undisclosed social-commerce/chat infrastructure
H1	GDPR Art. 5(1)(f), Art. 32	Eleven-year-old unpatched Android baseline
H2	GDPR Art. 13(1)(e)	Unnamed payment processor
H3	GDPR Art. 13(1)(c)	Undisclosed server-controlled capability surface

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to legal@temu.com, bcc Irish DPC/Austrian DSB/CERT.at/EDPB, 5 findings
2026-06-26/27	Follow-up, cc press@temu.com (address does not exist, bounced), pre-rebuts anticipated objections on controller identity and consent
2026-07-17 / 07-27 / 08-09	Further follow-ups; RFI-IRFOS self-corrects an earlier erroneous claim that legal@temu.com had bounced, which it never did
2026-08-18	Two follow-ups restate C1, cite the independent noyb complaint against Temu (January 2025)
2026-09-04	Final follow-up restates C1 as the sole still-open item, embargo reaffirmed unchanged
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Eight written notices across 90 days produced zero replies of any kind from legal@temu.com or Dispute@temu.com. All five findings, including the controller-identity discrepancy and the undisclosed social-commerce infrastructure, stand exactly as originally reported.

Residual Risk & Recommendations

- Accurately disclose the actual controller and processing entities for the com.baogong codebase, and publish the applicable Art. 46 transfer mechanism.
 - Disclose the social-commerce and chat infrastructure as a distinct processing activity with its own consent basis.
 - Raise minSdk from Android 6.0.
 - Name Braintree/PayPal as a payment processor.
 - Publish the documented capability surface of the ITpwContainerAPI WebView container.
 - Establish any working reply path at all: eight written notices over 90 days received zero acknowledgment of any kind.
-

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 Coordinated disclosure per ISO/IEC 29147. Research activity protected under Austria's Forschungsfreiheitsgesetz (Art. 17 StGG). GDPR Art. 5, 13, 32, 46. REF TEMU-2026-R1.