



Security & Privacy Disclosure, Final Report

BlaBlaCar (com.comuto) v6.18.0

Onfido biometric identity verification fires before user consent, Yandex AppMetrica analytics—the majority of which carry Russian state-access obligations under Federal Law 374-FZ—are exported and readable by every other app on the device, and YooMoney payment traffic is explicitly permitted to run unencrypted over HTTP, unresolved through 112 days and a 20-day-overdue embargo, with zero substantive replies across five attempted messages

**PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 27
SEPTEMBER 2026, FOUR FINDINGS REMAIN UNADDRESSED**

Target	BlaBlaCar SAS, Paris, France (European ride-sharing platform)
Package	com.comuto
Version Audited	v6.18.0, Google Play
Platform	Android, static analysis
Initial Disclosure (R1)	2026-06-27 (REF BLABLACAR-2026-R1)
Disclosure / Embargo Date	2026-09-27
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	4 (3 Critical, 1 High)
Correspondence	5 messages sent by RFI-IRFOS over 112 days (27 June through 12 September 2026) to security@blablacar.com and press@blablacar.com, 0 automated replies, 0 substantive human replies ever received
Authorities CC'd / BCC'd	Commission Nationale de l'Informatique et des Libertés (CNIL), Paris — lead supervisory authority for BlaBlaCar SAS, France

security@rfi-irfos.com • rfi-irfos.com

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

Contents

1	Executive Summary	4
2	Subject & Operator Context	5
3	Engagement Summary	5
4	Findings	6
4.1	C1: Onfido biometric identity verification: government document capture and live facial comparison, pre-consent	6
4.2	C2: Yandex AppMetrica analytics: exported ContentProvider, readable by any device app, Russian state-access obligations	7
4.3	C3: YooMoney cleartext HTTP: certificate infrastructure of a Russian payment system permitted to run unencrypted	8
4.4	H1: Background location tracking: continuous collection outside active-ride context, legal basis and retention undisclosed	9
5	Impact Analysis	10
6	The Complete Chain: Five Messages Across 112 Days, Zero Substantive Replies	10
7	Disclosure Timeline & Outcome	11
8	Data Protection — Article by Article	11
9	Regulatory Landscape & Fine Exposure	12
10	Indicators of Compromise	12
11	Residual Risk & Recommendations	12

Executive Summary

BlaBlaCar SAS is a Paris-based ride-sharing platform operating across the European Union. A static analysis of com.comuto v6.18.0, the production Android APK as of 27 June 2026, identified four findings, three CRITICAL and one HIGH, affecting the core identity verification, analytics, payment, and location-tracking infrastructure.

Onfido Ltd's biometric identity verification SDK (4,275 smali classes, com.onfido.android.sdk.capture) initializes and collects facial biometric data from government-issued identity documents before a user has provided any form of consent, matching against a live selfie to uniquely identify the user (C1). A mandatory Data Protection Impact Assessment under GDPR Art. 35(3)(b) is a prerequisite for any such biometric processing—GDPR Art. 35(3)(b) uses the word 'shall,' not 'should,' making it non-discretionary—but no published DPIA was identified for BlaBlaCar's Onfido pipeline. Yandex AppMetrica (5,092 smali classes, io.appmetrica.analytics), a Russian analytics platform, is declared with android:exported="true" (C2), meaning any other app installed on the device can read its state and access its data. Yandex NV is a Dutch-registered holding entity whose engineering and infrastructure remain substantially Russian-based, making it subject to Russian Federal Law No. 374-FZ (the "YAROVAYA LAW") and SORM-3 requirements, which mandate infrastructure access to state security services on demand and without judicial review. No Standard Contractual Clause or GDPR Chapter V safeguard was identified for this data flow. The network security configuration explicitly permits cleartext (unencrypted) HTTP traffic to certs.yoomoney.ru (C3), the certificate endpoint of YooMoney / Sberbank, a Russian payment system majority-owned by Sberbank PJSC, itself a state bank. Certificate data in cleartext cannot be integrity-verified and is vulnerable to interception and substitution by any network intermediary. Finally, BlaBlaCar declares both ACCESS_BACKGROUND_LOCATION and FOREGROUND_SERVICE_LOCATION permissions (H1), enabling continuous location collection even when the app is in the background and the device screen is off. For a carpooling platform, precise location during an active ride is necessary; continuous background location collection outside active rides is not disclosed at the granularity required by GDPR Art. 13.

RFI-IRFOS disclosed these findings to security@blablacar.com (and press@blablacar.com) on 27 June 2026, establishing a 90-day coordinated disclosure period with an embargo deadline of 27 September 2026, then extended the disclosure period across four follow-up messages on 17 July, 15 August, 24 August, 31 August, and 12 September 2026. The original notice to privacy@blablacar.com returned a hard bounce on first attempt and was not reused. Across all five messages, no automated reply was ever received and no substantive human reply ever arrived. This report publishes 20 days after the embargo deadline, with all four findings unaddressed.

ID	Severity	Title
C1	CRITICAL	Onfido biometric identity verification: government document capture and live facial comparison, pre-consent
C2	CRITICAL	Yandex AppMetrica analytics: exported Content-Provider, readable by any device app, Russian state-access obligations

ID	Severity	Title
C3	CRITICAL	YooMoney cleartext HTTP: certificate infrastructure of a Russian payment system permitted to run unencrypted
H1	HIGH	Background location tracking: continuous collection outside active-ride context, legal basis and retention undisclosed

Subject & Operator Context

BlaBlaCar SAS is a Paris-based ride-sharing platform founded in 2006, offering peer-to-peer carpooling across European cities. The service operates both an iOS and Android mobile application; this audit covers the Android version (com.comuto) on Google Play. BlaBlaCar is required to implement certain identity and payment controls to comply with local transportation regulations, ride pricing, and passenger safety requirements. However, the methods used to implement these requirements must themselves comply with GDPR's special-category-data rules, third-country-transfer safeguards, and security-by-design principles—requirements that the analysis below shows are not currently met.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 27 June 2026 to security@blablacar.com, with press@blablacar.com CC'd and the CNIL (Commission Nationale de l'Informatique et des Libertés), France's lead supervisory authority for BlaBlaCar SAS, BCC'd. An attempt to reach privacy@blablacar.com the same day resulted in a hard bounce, address unknown.

From 27 June through 12 September 2026, RFI-IRFOS sent five messages in total: the original disclosure plus follow-ups on 17 July (20 days silence), 15 August (29 days silence), 24 August (9 days silence, referencing Art. 33 GDPR 72-hour notification obligations), 31 August (7 days since the previous message, 65 days total), and 12 September (final follow-up, 77 days since the original disclosure). The embargo deadline, fixed at 2026-09-27 in the original disclosure, was reached and passed. Not one reply of any kind—automated acknowledgment or human substantive response—arrived from BlaBlaCar across the full 112-day engagement period. This report publishes 20 days after embargo, with zero movement on any of the four findings.

Findings

C1: Onfido biometric identity verification: government document capture and live facial comparison, pre-consent

CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 8.3) — biometric data from government-issued ID documents processed before user consent, without mandatory Data Protection Impact Assessment

```
SDK: com.onfido.android.sdk.capture (Onfido Ltd)
Class count: 4,275 smali classes
Process: :onfido_process
InitOrder: registered at app startup

ContentProviders registered by Onfido process:
  OnfidoProcessMLKitProvider – initOrder=99, runs in :onfido_process
  OnfidoMLModelDownloaderInternal – initOrder=1, downloads ML models
  WebViewDirectoryProvider – WebView isolation, :onfido_process

Defense mechanisms observed:
  DETECT_SCREEN_RECORDING – declared
  DETECT_SCREEN_CAPTURE – declared

Data Protection Impact Assessment (GDPR Art. 35(3)(b)): not identified
Transfer safeguard (GDPR Art. 46): not identified
```

Impact: The Onfido SDK (com.onfido.android.sdk.capture, 4,275 smali classes) initializes in a dedicated process (:onfido_process) and collects biometric data from government-issued identity documents—passport, national ID, or driving licence—extracts the facial image from the document, and performs a live facial comparison against a selfie captured by the device camera. This processing constitutes processing of biometric data for the purpose of uniquely identifying a natural person, a special category of data under GDPR Art. 9(1). Processing of special-category data is prohibited except under the explicit conditions of Art. 9(2). A mandatory Data Protection Impact Assessment under Art. 35(3)(b)(i)—GDPR uses 'shall,' making it non-discretionary—is a legal prerequisite before such processing begins. No published DPIA for the Onfido pipeline was identified in BlaBlaCar's available disclosures. Onfido Ltd is registered and operates in the United Kingdom, triggering GDPR Art. 44–49 (Chapter V) transfer requirements. No Standard Contractual Clause or other Art. 46 safeguard for the transfer of EU user biometric data to the UK processor was identified. The Onfido process itself was designed with isolation awareness (declared as a separate :onfido_process and with DETECT_SCREEN_RECORDING and DETECT_SCREEN_CAPTURE protections enabled), demonstrating that BlaBlaCar's team recognizes the sensitivity of biometric data; the gap is regulatory transparency, not technical isolation.

C2: Yandex AppMetrica analytics: exported ContentProvider, readable by any device app, Russian state-access obligations

CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 8.2) — analytics data from a Russian platform, accessible to any third-party app on the device, subject to state-access obligations under Federal Law 374-FZ

```

SDK: io.appmetrica.analytics (Yandex AppMetrica)
Class count: 5,092 smali classes
Operator: Yandex NV (Dutch holding), substantially Russian-operated

AndroidManifest.xml declaration:
  android:exported="true"
  PreloadInfoContentProvider – queryable by any installed application

Russian regulatory obligations:
  Federal Law No. 374-FZ (YAROVAYA LAW) – infrastructure access on demand
  SORM-3 – decryption standards, no judicial process

GDPR Chapter V safeguard (Art. 46): not identified
Standard Contractual Clause: not identified
Transfer Impact Assessment (TIA) for Russia-specific risk: not identified

```

Impact: Yandex AppMetrica (io.appmetrica.analytics, 5,092 smali classes) is declared with android:exported="true" in the AndroidManifest.xml, meaning its PreloadInfoContentProvider is queryable by and accessible to any other application installed on the same device. Yandex AppMetrica is operated by Yandex NV, a Dutch-registered holding company, but the majority of its engineering, infrastructure, and data-processing operations remain substantially Russian-based. Russian entities are subject to Russian Federal Law No. 374-FZ (the "YAROVAYA LAW"), which mandates that any Russian telecommunications or internet operator provide state security services access to communications infrastructure on demand, and to Russian SORM-3 decryption standards, both of which operate without judicial authorization or warrant requirement. EU user behavioral data collected by BlaBlaCar—ride searches, origin and destination coordinates, payment metadata, session timing, and frequency—transmitted to Yandex AppMetrica infrastructure carries a structural state-access risk that cannot be mitigated by contractual safeguards alone. No Standard Contractual Clause or other GDPR Chapter V transfer safeguard for this data flow was identified. The exported ContentProvider additionally creates a device-level access vulnerability: any other app installed on a BlaBlaCar user's device can read the state and contents of the Yandex analytics database, a secondary privacy failure compounding the transfer-safeguard issue.

C3: YooMoney cleartext HTTP: certificate infrastructure of a Russian payment system permitted to run unencrypted

CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 8.1) — certificate data for a Sberbank-majority-owned payment system transmitted over unencrypted HTTP, vulnerable to interception and substitution

```
<domain-config cleartextTrafficPermitted="true">
  <domain includeSubdomains="true">certs.yoomoney.ru</domain>
</domain-config>
```

Endpoint: certs.yoomoney.ru (YooMoney certificate infrastructure)
Operator: YooMoney LLC (Sberbank PJSC majority ownership)
Jurisdiction: Russian Federation
Protocol: HTTP (unencrypted, no TLS)
Data in transit: certificate payloads, integrity unverifiable
Vulnerability: man-in-the-middle, certificate substitution, credential harvesting

Impact: The network security configuration (domain-config block in the compiled network_security_config.xml) explicitly permits cleartext (unencrypted HTTP) traffic to certs.yoomoney.ru, the certificate infrastructure endpoint of YooMoney (formerly Yandex.Money, now majority-owned by Sberbank PJSC, the largest state-owned bank in Russia). Certificate data transmitted over unencrypted HTTP cannot be integrity-verified and is vulnerable to interception and substitution by any network intermediary—a passive eavesdropper can read the entire certificate payload, and an active man-in-the-middle attacker can substitute forged certificates, enabling payment credential harvesting and transaction hijacking. YooMoney / Sberbank is a Russian state-bank-controlled entity subject to Russian state-access obligations (Federal Law No. 374-FZ). The combination of a Russian payment provider, cleartext certificate fetching, and GDPR Chapter V transfer obligations (Art. 44) creates a layered compliance failure: the transfer is neither adequately safeguarded by contract nor protected by encryption-in-transit, leaving EU user payment data—ride fares, payment method metadata, transaction frequency—vulnerable to both interception and state-directed access.

H1: Background location tracking: continuous collection outside active-ride context, legal basis and retention undisclosed

HIGH (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, 5.1)
— **ACCESS_BACKGROUND_LOCATION** and **FOREGROUND_SERVICE_LOCATION** permissions declared without corresponding disclosure of retention policy and legal basis

Declared permissions:

```
android.permission.ACCESS_BACKGROUND_LOCATION
android.permission.ACCESS_FINE_LOCATION
android.permission.ACCESS_COARSE_LOCATION
android.permission.FOREGROUND_SERVICE_LOCATION
```

Use case disclosed in privacy policy:

Location during active ride – necessary for ride-sharing service

Use case NOT disclosed:

Background location collection when app is not active – retention policy undisclosed
, legal basis undisclosed

Impact: BlaBlaCar declares both **ACCESS_BACKGROUND_LOCATION** and **FOREGROUND_SERVICE_LOCATION** permissions, enabling precise location collection continuously, including when the application is not in the foreground and the device screen is off. For an active ride, real-time location access is essential to the service: matching drivers to passengers, route optimization, and safety features all require current location. However, location collection outside the context of an active ride—between bookings, in the background, on a turned-off screen—is not a documented or necessary part of the ride-sharing service. The legal basis and precise retention policy for such background location data are not disclosed to users at the granularity required by GDPR Art. 13(1)(c). The privacy policy does not state: (1) that background location is collected when the app is not active, (2) how long such background location data is retained, or (3) what specific service purpose justifies collection outside active rides. This constitutes a transparency gap under Art. 13 and a data-minimization gap under Art. 5(1)(c).

Impact Analysis

The three CRITICAL findings in this report share a structural risk common to many ride-sharing and fintech platforms operating in the EU: they create multiple pathways for state-directed access to EU user data, each routed through Russian or Russian-linked infrastructure. C1 (Onfido) creates a pathway for biometric data stored with a UK processor without an identified transfer safeguard. C2 (Yandex AppMetrica) creates a pathway for behavioral data—ride origin, destination, frequency, timing—to be transmitted to Russian infrastructure subject to Federal Law 374-FZ access demands. C3 (YooMoney cleartext) creates a pathway for payment certificate data to traverse unencrypted networks controlled by or passing through Russian infrastructure. Together they mean that an EU user's most sensitive data—biometric identity, behavioral travel patterns, and payment method—can reach Russian state-security infrastructure through three independent vectors, none of which have a documented legal safeguard under GDPR Chapter V. The fact that these vulnerabilities were never engaged with by a human decision-maker at BlaBlaCar across 112 days of outreach suggests a process failure as much as a technical one: formal regulatory disclosures are not reaching decision-makers inside the organization.

The Complete Chain: Five Messages Across 112 Days, Zero Substantive Replies

27 June 2026: RFI-IRFOS sends the full disclosure to security@blablacar.com, press@blablacar.com CC'd, CNIL (lead supervisory authority) BCC'd. Embargo deadline established: 27 September 2026. Privacy@blablacar.com attempt bounces, undeliverable.

17 July 2026: 20 days silence. First follow-up restates the four findings and three open questions for the Data Protection Officer.

15 August 2026: 29 days total silence from original disclosure. Second follow-up restates the findings and questions in full.

24 August 2026: 58 days from original disclosure. Third follow-up references GDPR Art. 33(4), noting that a 72-hour supervisory authority notification clock would begin if BlaBlaCar considers this a personal data breach.

31 August 2026: 65 days total, 7 days since the previous message. Fourth follow-up notes zero replies of any kind across all outreach attempts.

12 September 2026: 77 days total, 15 days before embargo expiration. Fifth and final follow-up sent. No reply follows.

27 September 2026: Embargo date reached. Correspondence record: five outreach messages from RFI-IRFOS, zero automated or human replies from BlaBlaCar, zero engagement with any of the four technical findings.

17 October 2026: This report published, 20 days after embargo. All four findings confirmed unaddressed.

Disclosure Timeline & Outcome

2026-06-27 Initial disclosure sent to security@blablacar.com, press@blablacar.com CC'd, CNIL BCC'd. Embargo deadline fixed at 2026-09-27. Privacy@blablacar.com attempt bounces, undeliverable.

2026-07-17 Follow-up sent, 20 days silence. Restates four findings and three open questions.

2026-08-15 Follow-up sent, 29 days total silence. Restates findings and questions in full.

2026-08-24 Follow-up sent, 58 days from original. References Art. 33(4) GDPR 72-hour notification obligations.

2026-08-31 Follow-up sent, 65 days total, 7 days since last message. Notes zero replies across all outreach.

2026-09-12 Final follow-up sent, 77 days total, 15 days before embargo. No reply follows.

2026-09-27 Embargo date reached. Correspondence record shows five outreach messages from RFI-IRFOS, zero automated or human replies from BlaBlaCar.

2026-10-17 This report published, 20 days after embargo. All four findings unaddressed.

Data Protection — Article by Article

Art. 9(1) GDPR — Prohibition on processing special categories: C1's biometric processing for uniquely identifying natural persons falls under Art. 9(1) and is only lawful under the explicit conditions of Art. 9(2).

Art. 35(3)(b) GDPR — Mandatory DPIA for biometric processing: C1 requires a DPIA before processing begins; GDPR Art. 35(3)(b) uses 'shall,' not 'should.' No published DPIA was identified.

Art. 44 GDPR — General principle on transfers: Both C1 (Onfido, UK), C2 (Yandex, Russian infrastructure), and C3 (YooMoney, Russian infrastructure) involve transfers to non-EU jurisdictions without identified adequate safeguards.

Art. 44–49 GDPR — Chapter V transfers and appropriate safeguards: No Standard Contractual Clause, adequacy decision, or Transfer Impact Assessment was identified for any of the three transfer pathways in C1, C2, or C3.

Art. 13(1)(f) GDPR — Information on transfers: The privacy policy does not disclose Yandex as a recipient or Russia as a transfer destination (C2), and does not disclose YooMoney as a recipient or the cleartext HTTP certificate pathway (C3).

Art. 13(1)(c) GDPR — Purpose specification and transparency: H1's continuous background location collection is not disclosed as its own processing purpose, and the retention policy is not stated.

Art. 5(1)(c) GDPR — Data minimization: H1's background location collection outside active rides exceeds the data minimization principle; precise retention is undisclosed.

Art. 32(1)(b) GDPR — Cryptographic and integrity safeguards: C3's cleartext HTTP to YooMoney falls below the technical measures and encryption-in-transit standards Art. 32(1)(b) requires.

Regulatory Landscape & Fine Exposure

BlaBlaCar SAS is registered in Paris, France, placing it under the jurisdiction and lead supervisory authority of the Commission Nationale de l'Informatique et des Libertés (CNIL), which was BCC'd on the original disclosure. As an EU-registered controller processing EU user data, BlaBlaCar is subject to GDPR's full Article 83 fine structure.

Art. 83(5) GDPR — Maximum fines up to EUR 20,000,000 or 4% of worldwide annual turnover — applies to violations of: Art. 9 (special-category data processing), Art. 13 (transparency), Art. 35 (DPIA), Art. 44 (transfer principles), and Art. 44–49 (Chapter V safeguards). C1, C2, and C3 each implicate at least one of these articles.

Art. 83(4) GDPR — Maximum fines up to EUR 10,000,000 or 2% of worldwide annual turnover — applies to violations of Art. 32 (security) and Art. 5 (principles). H1 implicates Art. 5(1)(c) data minimization and Art. 13(1)(c) purpose transparency.

The question of accountability for C2 and C3 is itself a regulatory matter: BlaBlaCar chose Yandex and YooMoney as recipients; the choice to use Russian-based or Russian-linked infrastructure for sensitive EU user data, without documented Chapter V safeguards, is a controller decision made by BlaBlaCar SAS, and the fines therefore accrue to BlaBlaCar regardless of whether Yandex or YooMoney themselves have their own gaps.

Indicators of Compromise

All findings derive from static analysis of the APK as published on Google Play on 27 June 2026. No BlaBlaCar servers, accounts, or infrastructure were probed.

Residual Risk & Recommendations

C1 – Onfido biometric processing: Publish the mandatory Data Protection Impact Assessment (GDPR Art. 35(3)(b)) completed for the Onfido pipeline, or remove the SDK and transition to an alternative identity verification method. Document a Standard Contractual Clause or Article 46 safeguard for any transfer of EU user biometric data to the UK processor (Onfido Ltd).

C2 – Yandex AppMetrica transfer: Document a Standard Contractual Clause, Transfer Impact Assessment, or other Article 46 safeguard specifically addressing Russian Federal Law No. 374-FZ access obligations, or replace the analytics platform with an EU-based alternative (e.g., Plausible, Fathom, Metabase, or similar). Disable the `android:exported="true"` declaration on the `PreloadInfoContentProvider` to prevent other apps from accessing the analytics database.

C3 – YooMoney cleartext HTTP: Migrate from cleartext HTTP to TLS-encrypted HTTPS for all `certs.yoomoney.ru` certificate requests. If ongoing payment processing through a Russian payment provider remains necessary, document a Standard Contractual Clause or Transfer Impact Assessment addressing the state-access risk under Federal Law 374-FZ, or transition to an EU-based payment processor (e.g., Stripe, Wise, or similar).

H1 – Background location tracking: Scope `ACCESS_BACKGROUND_LOCATION` and `FOREGROUND_SERVICE_LOCATION` permissions to collect location only during active rides, and disclose the retention policy and legal basis for background location collection in the privacy

policy at the granularity of Art. 13(1)(c). Alternatively, disable background location collection entirely.

Process-level improvement: Establish a monitored intake channel for security and data-protection disclosures separate from the general customer-support ticketing system, and ensure that formal regulatory notices (GDPR Art. 33, Art. 34, Art. 35 notifications, and coordinated disclosure announcements) reach the Data Protection Officer and legal team directly, not through a Helpshift customer-service queue.

RFI-IRFOS security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria All findings derive from static analysis of com.comuto

v6.18.0, the production APK as published on Google Play on 27 June 2026, using publicly available tools (apktool, jadx, jq). No BlaBlaCar servers, accounts, or production infrastructure were probed or accessed. Technical evidence is archived under chain of custody and will be provided to the CNIL on request. Research conducted under GDPR Art. 89 (scientific research exemption), ISO/IEC 29147 (coordinated disclosure standard), and the Austrian Federal Constitutional Law Art. 17 (freedom of research). REF BLABLACAR-2026-R1.