Coordinated Security & Privacy Disclosure, Final Report

Match Group: Tinder, Hinge, OkCupid, Plenty of Fish, BLK

Five-app dating platform portfolio audit, one shared biometric and security architecture

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY-ONE DAYS, EIGHTEEN WRITTEN NOTICES, ZERO SUBSTANTIVE REPLIES

Target	Match Group, Inc., Dallas, Texas, US (NASDAQ: MTCH)
Products audited	Tinder (com.tinder) 17.21.0, Hinge (co.hinge.app) 9.126.1, OkCupid (com.okcupid.okcupid) 113.3.0, Plenty of Fish (com.pof.android) 5.66.0, BLK (com.affinityapps.blk) 12.9.0
Disclosure reference	REF MATCHGROUP-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (MG-01 FaceTec / MG-03 BLK-TikTok / MG-05 Incognia, CVSS v4.0 8.7 High)

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 Architecture & Data Flow: A Shared Pattern, Not Five Coincidences 4

4 Findings 5

4.1 MG-01: FaceTec biometric verification confirmed group-wide: five for five audited apps . . . 5

4.2 MG-02: OkCupid: production UI string names five GDPR Art. 9 categories for cross-brand commercial profiling . . . 5

4.3 MG-03: BLK: TikTok Open SDK (ByteDance) bridges a racial-origin-defined userbase to Chinese infrastructure . . . 6

4.4 MG-04: Hinge: private messages routed through SendBird, stored unencrypted on US servers . . . 6

4.5 MG-05: Hinge: Incognia location behavioral fingerprinting reveals sensitive venue visits . . . 7

4.6 MG-06: Tinder: LiveRamp data broker SDK links dating and sexual-orientation signals to global ad identity . . . 7

4.7 MG-07: Tinder: Meta SDK creates a sexual-behavior-signal pipeline to Meta's ad-targeting system . . . 8

4.8 MG-08: Systemic transport security failure: no certificate pinning, cleartext HTTP permitted by default (OkCupid) . . . 8

4.9 MG-09: Hardcoded Firebase API keys confirmed in all five audited apps . . . 9

4.10 MG-10: Plenty of Fish: READ_PHONE_STATE grants IMEI access, unique among the audited portfolio . . . 9

4.11 MG-11: BLK: Match Group internal IP address and cleartext corporate domain hardcoded in production NSC . . . 10

5 Impact Analysis 10

6 Data Protection, Article by Article 11

7 Regulatory & Legal Landscape 12

8 Additional Findings by App 12

9 Disclosure Timeline & Outcome 12

10 Residual Risk & Recommendations 13

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of five Match Group dating applications: Tinder, Hinge, OkCupid, Plenty of Fish, and BLK. Across the five apps, 32 findings were identified. The findings below are organized around the patterns that recur across the portfolio rather than as five separate, unrelated app audits, because the evidence shows a shared group-level architecture, not five independent engineering decisions.

The FaceTec biometric verification SDK, transmitting 3D facial liveness data to a US server with no visible transfer safeguard, was confirmed in every one of the five audited apps, five for five. Hardcoded Firebase credentials were likewise found in all five. OkCupid's production interface contains a consent toggle that explicitly names five GDPR Article 9 special categories, sexual orientation, race, ethnicity, religion, and political belief, for use in cross-brand commercial profiling across the Match Group portfolio, a finding RFI-IRFOS's own research series describes as its most legally significant to date. BLK, a platform built specifically for Black singles, integrates a ByteDance-owned TikTok SDK, creating a data bridge between a userbase whose defining shared attribute is racial origin and Chinese platform infrastructure with no EU adequacy framework.

Eighteen written notices were sent to Match Group over 91 days. None produced a substantive reply. The findings below stand exactly as originally reported.

Scope: Static analysis of the publicly downloaded production Android APKs for five Match Group applications. No Match Group backend, account, or infrastructure was accessed or tested.

Disposition

Five separate R1 notices were sent on 20 June 2026, one per app, to security@matchgroup.com and privacy@matchgroup.com, bcc Austrian DSB and CERT.at: Tinder (8 findings), Hinge (7), OkCupid (6), Plenty of Fish (5), BLK (6), 32 findings in total. Follow-ups were consolidated into a single five-app thread and repeated on 29 August, 4 September, and three times on 12 September 2026. Across 91 days and eighteen written messages, Match Group produced no substantive reply of any kind. The FaceTec biometric SDK was independently confirmed in all five apps audited, five for five.

ID	Severity	Title
MG-01	CRITICAL	FaceTec biometric verification confirmed group-wide: five for five audited apps
MG-02	CRITICAL	OkCupid: production UI string names five GDPR Art. 9 categories for cross-brand commercial profiling
MG-03	CRITICAL	BLK: TikTok Open SDK (ByteDance) bridges a racial-origin-defined userbase to Chinese infrastructure
MG-04	CRITICAL	Hinge: private messages routed through SendBird, stored unencrypted on US servers

ID	Severity	Title
MG-05	CRITICAL	Hinge: Incognia location behavioral fingerprinting reveals sensitive venue visits
MG-06	CRITICAL	Tinder: LiveRamp data broker SDK links dating and sexual-orientation signals to global ad identity
MG-07	CRITICAL	Tinder: Meta SDK creates a sexual-behavior-signal pipeline to Meta's ad-targeting system
MG-08	CRITICAL	Systemic transport security failure: no certificate pinning, cleartext HTTP permitted by default (OkCupid)
MG-09	HIGH	Hardcoded Firebase API keys confirmed in all five audited apps
MG-10	HIGH	Plenty of Fish: READ_PHONE_STATE grants IMEI access, unique among the audited portfolio
MG-11	HIGH	BLK: Match Group internal IP address and cleartext corporate domain hardcoded in production NSC

Subject & Operator Analysis

Match Group, Inc. (NASDAQ: MTCH, Dallas, Texas) operates a portfolio of dating platforms including Tinder, Hinge, OkCupid, Plenty of Fish, and BLK, among others, serving EU residents and therefore falling within GDPR's extraterritorial scope under Art. 3(2). RFI-IRFOS's audit covered five of these apps; the 20 June 2026 correspondence noted that the same architecture likely extends to the remainder of the portfolio (OurTime, Chispa, The League, Archer), which were not independently audited and are not the subject of this report's findings.

Architecture & Data Flow: A Shared Pattern, Not Five Coincidences

- FaceTec biometric verification: confirmed in all five audited apps, transmitting facial liveness data to the same US endpoint (MG-01).
- Hardcoded Firebase credentials: confirmed in all five audited apps, each pointing to a distinct project (MG-09).
- Absent or bypassable transport security: no certificate pinning in Tinder, Hinge, and Plenty of Fish; cleartext HTTP permitted by default in OkCupid (MG-08).
- Cross-brand infrastructure: com.mtch.coe.profiletransfer and com.mtch.coe.mercury, Match Group Center of Excellence namespaces, confirmed active in both OkCupid and BLK, technical infrastructure for moving user profiles between brands.
- App-specific additions on top of the shared base: SendBird message storage and Incognia location fingerprinting (Hinge), LiveRamp and Meta SDKs (Tinder), a TikTok/ByteDance SDK (BLK), and IMEI-level device access (Plenty of Fish).

Findings

MG-01: FaceTec biometric verification confirmed group-wide: five for five audited apps

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

The FaceTec SDK (com.facetec.sdk), transmitting 3D facial liveness data to api.facetec.com/api/v3.1/biometrics/liveness-3d (US), was independently confirmed in Tinder (1,093 classes), Hinge, OkCupid (1,135 classes), Plenty of Fish, and BLK.

No response was received naming this finding. This is not an isolated per-app SDK choice: it is a group-level biometric processing programme spanning the entire audited portfolio, transmitting EU users' facial geometry, GDPR Art. 9(1) special category data, to a US company with no visible standard contractual clause or adequacy mechanism in any of the five binaries. On BLK specifically, every user completing liveness verification has two Art. 9 categories processed simultaneously: biometric data and racial origin, the platform's own defining characteristic. No group-level Data Protection Impact Assessment covering this intersection is evident from any of the five apps or the correspondence.

Impact: EU users across five separate dating platforms have 3D facial biometric data transmitted to a US processor with no visible cross-border transfer safeguard, a group-wide pattern rather than an isolated app defect.

Fix: Conduct a single group-level DPIA covering FaceTec's use across the full Match Group portfolio, implement a valid Art. 44-49 transfer mechanism, and obtain explicit Art. 9(2)(a) consent specific to biometric processing, separate from general account creation consent.

MG-02: OkCupid: production UI string names five GDPR Art. 9 categories for cross-brand commercial profiling

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

res/values/strings.xml, verbatim: "If this toggle is on, your sensitive personal data (e.g. sexual orientation, race, ethnicity, religion, political beliefs) will be used to tailor your Match Group Offers."

No response was received naming this finding. This is not a misconfiguration to be patched; it is a documented product decision, found in the shipped production interface itself. OkCupid collects sexual orientation with more than 40 granular options, making this the most sensitive Art. 9 dataset RFI-IRFOS has documented in its dating-app research series. A single toggle covering five distinct special categories at once, for cross-brand commercial use, does not meet the specificity and granularity GDPR Art. 9(2)(a) requires. The CVSS score is scored on demonstrated confidentiality impact and is lower than the qualitative label reflects; the report keeps the CRITICAL label because this is, in RFI-IRFOS's own assessment across its full audit series, the most legally significant single finding on record: a company's own shipped product text describing exactly the processing GDPR Art. 9 exists to constrain.

Impact: Users' sexual orientation, racial origin, ethnicity, religion, and political beliefs can be used for cross-brand commercial profiling across the Match Group portfolio under a single, non-granular consent toggle.

Fix: Replace the single toggle with per-category, specific, granular consent meeting GDPR Art. 9(2)(a), and confirm in writing that cross-brand use of this data has stopped until that consent architecture exists.

MG-03: BLK: TikTok Open SDK (ByteDance) bridges a racial-origin-defined userbase to Chinese infrastructure

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

com.bytedance.sdk.open.tiktok is integrated into BLK, an app built specifically for Black singles, where racial and ethnic origin is the platform's organizing characteristic.

No response was received naming this finding. ByteDance is subject to China's Cybersecurity Law and Personal Information Protection Law. Whether via social login or content sharing, this SDK creates a data bridge between a userbase whose shared Art. 9 attribute is racial origin and Chinese platform infrastructure, with no EU adequacy decision and no meaningful protection against Chinese state access obligations. This is the only Chinese SDK finding across RFI-IRFOS's Match Group series, and in combination with the platform's demographic focus, the most politically sensitive Art. 9 exposure in the report.

Impact: Racial origin data, inherent to using a platform built for Black singles, is bridged to Chinese infrastructure subject to state access laws with no EU transfer safeguard.

Fix: Remove the TikTok Open SDK or implement a verified Art. 44-49 transfer mechanism specific to this data flow, and disclose the ByteDance data relationship explicitly to BLK users.

MG-04: Hinge: private messages routed through SendBird, stored unencrypted on US servers

HIGH, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.2

com.sendbird.sdk.messaging.* confirms Hinge's real-time chat runs on SendBird, a US company. SendBird does not provide end-to-end encryption by default, meaning message content is accessible to SendBird at rest.

No response was received naming this finding. Intimate conversations between Hinge users transit and are stored on a third-party US entity's servers, with no disclosure of this fact visible in Hinge's own interface. The CVSS score reflects that reading this content requires access to SendBird's own infrastructure (AT:P), a precondition rather than a direct client-side exposure, which is also why the report treats this as a serious but distinct risk class from Meta's Messenger key-custody finding in RFI-IRFOS's parallel Meta Platforms report: here the transport is not marketed as end-to-end encrypted in the first place, but users are not told a named third party holds their message content in readable form.

Impact: Private Hinge conversations are held in a form readable by a third-party US processor, undisclosed to users, with no independent encryption layer beyond whatever SendBird itself provides.

Fix: Disclose SendBird as the message-storage processor in Hinge's privacy notice, and implement end-to-end encryption or an equivalent architecture that removes SendBird's ability to read message content.

MG-05: Hinge: Incognia location behavioral fingerprinting reveals sensitive venue visits

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

The Incognia SDK (com.incognia, 2,149 classes) builds persistent behavioral fingerprints from GPS location history, with explicit ACCESS_FINE_LOCATION and ACCESS_BACKGROUND_LOCATION checks.

No response was received naming this finding. Continuous location tracking on a dating app can reveal home address, workplace, a partner's home, and visits to sensitive venues including sexual health clinics and LGBTQ+ spaces. Combined with Hinge's own dating profile data, sexual orientation and relationship goals, this builds a deeply intimate behavioral profile transmitted to a US-based processor with no EU adequacy decision covering transfer at this precision.

Impact: A user's real-world movements, including visits to sensitive locations, are fingerprinted and combined with their stated sexual orientation and relationship data, transmitted to a US third party.

Fix: Scope location collection to the minimum needed for core matching functionality, disclose Incognia's specific processing purpose separately from general location permissions, and cease inferring venue-level behavioral patterns.

MG-06: Tinder: LiveRamp data broker SDK links dating and sexual-orientation signals to global ad 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

LiveRamp ATS is integrated across 392 smali classes with a hardcoded configuration UUID. LiveRamp hashes email addresses into persistent 'RampIDs' shared across its commercial data network.

```
LiveRampGeoOverride: {NONE, EU, US_CA, US_OTHER}
syncLiveRampWithConsent(...)
```

No response was received naming this finding. The APK's own LiveRampGeoOverride enum and syncLiveRampWithConsent method show Tinder is aware of jurisdictional differences in how this data flow should behave, yet the SDK ships active in the EU-distributed build with geo-behavior controlled server-side, meaning a misconfiguration or A/B test could enable full sharing for EU users with no code change. No GDPR Art. 9(2) legal basis applies to routing dating-preference and sexual-orientation signals through a commercial advertising data broker.

Impact: Tinder users' dating preferences and sexual orientation signals are linkable to their cross-web advertising identity via a persistent RampID, with EU behavior controlled remotely rather than fixed in the shipped code.

Fix: Remove EU users from LiveRamp's data flow at the code level, not via server-side geo-configuration alone, and publish the actual current EU behavior of syncLiveRampWithConsent.

MG-07: Tinder: Meta SDK creates a sexual-behavior-signal pipeline to Meta's ad-targeting system

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 Meta SDK occupies 3,583 class files in the Tinder APK. Tinder captures sexual orientation, relationship goals, and behavioral signals including swipe patterns and match rates.

No response was received naming this finding. For users who also hold a Facebook account on the same device, Meta can cross-reference Tinder behavioral data against their advertising profile, constructing a sexual behavior signal inside Meta's own ad-targeting infrastructure. No GDPR Art. 9(2) legal basis covers this data flow, and it raises a potential Art. 26 joint-controller relationship between Match Group and Meta that neither company's privacy notice appears to address.

Impact: Sexual orientation and dating-behavior signals from Tinder can be cross-referenced against a user's Meta advertising profile on the same device, without a documented Art. 9(2) basis or joint-controller disclosure.

Fix: Scope the Meta SDK integration to exclude behavioral and preference signals, or obtain specific Art. 9(2)(a) consent and publish a joint-controller arrangement with Meta covering this data flow.

MG-08: Systemic transport security failure: no certificate pinning, cleartext HTTP permitted by default (OkCupid)

HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 8.6

Tinder, Hinge, and Plenty of Fish ship network_security_config.xml trusting only the system CA store with no pins; OkCupid's base-config sets cleartextTrafficPermitted="true" for all domains outside a 5-domain whitelist.

No response was received naming this finding. This is a recurring pattern across the portfolio, not an isolated oversight in one app: every audited app trusts the full system CA store with no certificate pinning, and OkCupid goes further by permitting outright cleartext HTTP as the default for any non-whitelisted domain, including third-party SDKs like AppsFlyer, Arkose-Labs, and Firebase. On platforms explicitly storing sexual orientation, racial origin, religion, and political views, this is a categorical GDPR Art. 32(1)(a) failure across the group, not a single app's configuration error.

Impact: An attacker in a position to intercept traffic on a compromised network, an MDM-injected corporate root, or a compromised CA can intercept or manipulate FaceTec biometric uploads, private messages, and Art. 9 profile data across the Match Group portfolio with no client-side detection.

Fix: Implement certificate pinning with primary and backup pins across the full portfolio, and remove OkCupid's cleartext-permitted default, restricting it to an explicit, minimal allowlist if needed at all.

MG-09: Hardcoded Firebase API keys confirmed in all five audited apps

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

Firebase credentials hardcoded in res/values/strings.xml in Tinder, Hinge, OkCupid, Plenty of Fish, and BLK, each pointing to a distinct Firebase project. Several databases had been deactivated, but the credentials remained live in the shipped production APK regardless.

```
Tinder: AIzaSyD-LJICkfrnODTCsi7-MViTXwaA1QcuG04 (gotinder-com-api-project)
Hinge: AIzaSyB-apSzB00iSHaEIG-5nalT2DDVSAHcPXA (hinge-layer-prod)
OkCupid: AIzaSyB-bSz0R6lgc-rjoe9eRwlKf1rznVGxQj0 (api-project-832916845466)
POF: AIzaSyALpKZPc98fZSPNHDsYYCkocVHSLKaTJoM (pof-gcm)
BLK: AIzaSyDKAEfw65RP-JZgeHt_VvT8kvR85kWuIKA (blk-swipe)
```

No response was received naming this finding. Deactivating a database does not remove the exposure: the credentials still enable FCM token enumeration and auth probing against each app's backend, five for five, indicating a shared build process that does not rotate or remove credentials after a service migration.

Impact: Five separate Firebase credential sets remain live in shipped production APKs, enabling FCM token enumeration against each app's user base regardless of whether the originally paired database is still active.

Fix: Rotate all five keys, restrict each to its production certificate fingerprint, and add credential rotation to the standard deprecation process for any migrated Firebase service.

MG-10: Plenty of Fish: READ_PHONE_STATE grants IMEI access, unique among the audited portfolio

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

POF declares android.permission.READ_PHONE_STATE, granting access to IMEI, IMSI, phone number, and SIM state. This permission is absent from every other audited Match Group app.

No response was received naming this finding. IMEI is a persistent, non-resettable device identifier that survives app reinstalls and advertising-ID resets, unlike the identifiers the rest of the portfolio relies on. No legitimate purpose for IMEI-level access is apparent in a dating application's core function, and its presence in exactly one of five otherwise architecturally similar apps suggests it is not a considered, group-wide decision.

Impact: Plenty of Fish users are tracked via a persistent hardware identifier that survives resets other Match Group apps do not use, with no apparent functional justification.

Fix: Remove READ_PHONE_STATE unless a specific, documented purpose requires IMEI-level access, and align POF's identifier strategy with the rest of the portfolio.

MG-11: BLK: Match Group internal IP address and cleartext corporate domain hardcoded in production NSC

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

BLK's production network_security_config.xml declares a domain entry for the RFC 1918 private address 10.230.10.123 alongside match.corp, both with cleartextTrafficPermitted="true".

No response was received naming this finding. A private internal IP address belonging to Match Group's own network, shipped in a public production APK, discloses internal network topology to anyone who downloads the app, and cleartext HTTP is explicitly permitted from production app traffic to that internal domain.

Impact: Match Group's internal network topology is exposed via a public production APK, with cleartext HTTP permitted to a named internal domain from production app traffic.

Fix: Remove internal-network configuration entries from any production build's network_security_config.xml, and audit the build pipeline for how internal addresses reached a shipped artifact.

Impact Analysis

Dating platforms collect, by their nature, some of the most intimate categories of personal data GDPR Art. 9 exists to protect: sexual orientation, relationship intentions, and, on BLK, racial origin as the platform's organizing principle. The findings in this report do not describe a company failing to anticipate a novel risk. OkCupid's own production interface already names the special categories at stake, in plain language, next to a toggle controlling their commercial use across brands. Every structural safeguard this report finds missing, biometric transfer safeguards, certificate pinning, credential rotation, is a well understood, standard practice elsewhere in the industry; its absence here, repeated identically across five apps, describes a choice made at the group level, not an accident repeated five times independently.

BLK's TikTok/ByteDance integration deserves separate emphasis: a platform whose entire premise is serving a userbase defined by racial origin routes data through infrastructure operated by a company subject to a foreign government's cybersecurity and data access laws, with the demographic specificity of the platform itself narrowing exactly who is exposed.

Data Protection, Article by Article

Finding	Provision	Concern
MG-01	GDPR Art. 9(1), Art. 4(14), Art. 44-49	Group-wide biometric transfer to the US with no visible safeguard
MG-02	GDPR Art. 9(1), Art. 9(2)(a), Art. 5(1)(b)	Single non-granular consent toggle for five Art. 9 categories, cross-brand use
MG-03	GDPR Art. 9(1), Art. 44-49	Racial-origin-defined userbase bridged to Chinese SDK infrastructure
MG-04	GDPR Art. 5(1)(f), Art. 13(1)(e), Art. 44-49	Undisclosed third-party US message storage, not end-to-end encrypted
MG-05	GDPR Art. 9(1) (inferred), Art. 5(1)(c), Art. 44-49	Behavioral location fingerprinting revealing sensitive venues
MG-06, MG-07	GDPR Art. 9(2), Art. 26	Dating and sexual-orientation signals routed to commercial ad infrastructure
MG-08	GDPR Art. 32(1)(a)	No certificate pinning group-wide; cleartext HTTP by default (OkCupid)
MG-09, MG-10, MG-11	GDPR Art. 32, Art. 5(1)(c)	Credential hygiene, excess device identifiers, internal infrastructure exposure

Regulatory & Legal Landscape

This disclosure was bcc'd throughout to the Austrian Data Protection Authority (DSB) and CERT.at. Match Group's dating apps process GDPR Art. 9 special category data (sexual orientation, and on BLK, racial origin) at a scale and specificity that places the findings in this report squarely within DPA enforcement priorities already established against comparable platforms. No prior GDPR enforcement action against Match Group specific to these findings is asserted in this report; the findings are presented on their own technical and legal merits.

Additional Findings by App

Beyond the eleven findings detailed above, the following were confirmed and included in the original per-app disclosures. None received a response.

- Tinder: ACCESS_ADSERVICES_TOPICS deriving sexual-behavior-adjacent interest categories; RecommendProfileBroadcastReceiver exported without permission (CWE-284); READ_CONTACTS and BLUETOOTH scope undisclosed.
- Hinge: BrazeActionReceiver exported without permission (CWE-284); READ_CONTACTS upload scope for non-Hinge users undisclosed.
- OkCupid: ACCESS_ADSERVICES_TOPICS fed by explicitly stated sexual orientation, religion, and political views rather than inferred usage signals.
- BLK: ACCESS_ADSERVICES_TOPICS on a racial-origin platform; cross-brand profile transfer infrastructure (com.mtch.coe.profiletransfer.piertopier, com.mtch.coe.mercury) active alongside OkCupid's.

Disclosure Timeline & Outcome

Date	Event
2026-06-20	Five R1 notices sent, one per app (Tinder, Hinge, OkCupid, POF, BLK), bcc Austrian DSB/CERT.at
2026-08-29	Follow-up, 70 days, zero response, all five apps
2026-09-04	Follow-up, 76 days, zero substantive reply
2026-09-12	Three follow-up messages the same day, restating findings and Art. 33 reporting-window language, 84 days
2026-09-19	Embargo closes; this report publishes

Eighteen written notices across 91 days produced no substantive reply from Match Group. Every one of the 32 findings across five apps stands exactly as originally reported.

Residual Risk & Recommendations

- Conduct a single group-level DPIA for FaceTec covering all Match Group brands, not a per-app review.
- Redesign OkCupid's Art. 9 consent toggle into specific, granular, per-category consent before any cross-brand commercial use resumes.
- Remove or replace the TikTok/ByteDance SDK in BLK, or implement and publish a verified Art. 44-49 transfer mechanism.
- Disclose SendBird's role and message-retention model to Hinge users, and move toward an architecture that removes SendBird's own read access to message content.
- Scope Incognia's location collection to active, disclosed use cases rather than continuous behavioral fingerprinting.
- Implement certificate pinning group-wide and remove OkCupid's cleartext-permitted default.
- Rotate all five exposed Firebase credentials and add rotation to the standard service-deprecation process.
- Remove Plenty of Fish's READ_PHONE_STATE grant absent a specific, documented purpose.
- Audit the build pipeline that shipped Match Group's internal IP address in a public BLK release.

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. 4, 5, 6, 9, 13, 26, 32, 44-49. REF MATCHGROUP-2026-R1.