Coordinated Security & Privacy Disclosure, Final Report

Tipico Austria for Android (tipico.sports.at)

The largest biometric stack in this year's audit series, an undisclosed sub-processor chain routing liveness data between vendors, one thin acknowledgment in 91 days

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY-ONE DAYS, ONE THIN ACKNOWLEDGMENT, NO SUBSTANTIVE REPLY

Target	Tipico Co. Ltd., Malta (lead supervisory authority: IDPC Malta)
Product audited	Tipico Austria for Android, tipico.sports.at, v9.1.1
Disclosure reference	REF TIPICO-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 Firebase suite / C2 triple biometric stack, CVSS v4.0 9.3)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production Tipico Austria Android application and identified nine findings, two CRITICAL, seven HIGH. The most significant: a triple biometric stack, FaceTec, IDnow, and Unissey, totaling 3,206 smali classes, the largest biometric stack identified across this year's 31-app audit series. A specific code path confirms IDnow internally routes biometric liveness data to Unissey via WebSocket, an undisclosed sub-processor relationship never named in Tipico's privacy documentation, alongside NFC ePassport chip reading for both standard ICAO 9303 documents and UAE identity documents.

Separately, the production binary hardcodes a full eleven-module Firebase suite, the largest such suite identified in this audit series. Seven further findings raise separate concerns: FinTecSystems' XS2A Wizard providing direct PSD2 bank-account access as an undisclosed processor; SAP Emarsys geofencing that activates at device boot before the app is even opened, feeding a behavioral-prediction engine; LiveSwitch WebRTC with full-screen MediaProjection capture capability; IMEI collection alongside all-files device access with no disclosed purpose; IBM Instana capturing network metadata from biometric, banking, and betting transactions alike; and advertising-attribution identifiers operating on the same platform as biometric and banking data.

Nine written notices were sent over 91 days. The only reply received, from Tipico's press office on 16 July, was a single line acknowledging receipt, addressing none of the nine findings. No further reply of any kind followed. All nine findings stand exactly as originally reported.

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

Disposition

R1 sent 20 June 2026, first attempt bounced on an internal-only relay address that had leaked into public-facing correspondence, redelivered 28 June to compliance@tipico.com. Eight further written notices followed. presse@tipico.com sent one one-line receipt acknowledgment on 16 July, addressing none of the nine findings. No further reply of any kind was received.

ID	Severity	Title
C1	CRITICAL	Hardcoded Firebase production credentials, an eleven-module suite
C2	CRITICAL	Triple biometric stack across three countries, undisclosed sub-processor chain between vendors
H1	HIGH	FinTecSystems XS2A Wizard: direct PSD2 bank-account access, undisclosed processor
H2	HIGH	IDnow NFC ePassport chip reading: immutable government-issued biometric data

ID	Severity	Title
H3	HIGH	SAP Emarsys geofencing activates at device boot, feeds a behavioral-prediction engine
H4	HIGH	LiveSwitch WebRTC with full-screen MediaProjection capture capability
H5	HIGH	IMEI collection alongside all-files device access, no disclosed purpose
H6	HIGH	IBM Instana: undisclosed network metadata capture from biometric, banking, and betting transactions
H7	HIGH	Advertising-attribution identifiers on a biometric and banking platform

Subject & Operator Analysis

Tipico Co. Ltd., licensed in Malta, operates Austrian sports betting under the Austrian Gluecksspielgesetz, with Malta's IDPC as lead GDPR supervisory authority.

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: Hardcoded Firebase production credentials, an eleven-module suite

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 9.3

A complete Firebase project configuration is extracted verbatim from res/values/strings.xml, with eleven active Firebase modules: Analytics, Crashlytics, Auth, Storage, Messaging, Performance, Remote Config, App Check, A/B Testing, Sessions, and Installations, the largest Firebase suite identified across this audit series.

```
API Key:  AIzaSyDbU8uCQbulTy_eu4YqRt_Lja-JiSF_-ng
App ID:   1:542174116933:android:4baf15064d3d6ad715772c
DB URL:   https://tipico-ad815.firebaseio.com
Project:  tipico-ad815
```

No response was received naming this finding. The credential is extractable from the public Play Store binary in under 60 seconds.

Impact: A publicly extractable credential covering an eleven-module Firebase suite enables broad probing across authentication, storage, remote configuration, and analytics infrastructure.

Fix: Rotate the credential, restrict it to the production certificate fingerprint, and audit security rules across all eleven active modules.

C2: Triple biometric stack across three countries, undisclosed sub-processor chain between vendors

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

FaceTec Inc. (US, 1,129 classes), IDnow GmbH (Germany, 1,844 classes), and Unissey SAS (France, 233 classes) together total 3,206 smali classes, the largest biometric stack identified in this audit series.

```
com/facetec/sdk/                          <- biometric liveness, FaceTec Inc. (US)
de/idnow/                                 <- AI video ident + NFC ePassport, IDnow
     GmbH (DE)
com/unissey/sdk/                          <- facial liveness detection, Unissey
    SAS (FR)
de/idnow/ai/websocket/unissey/            <- IDnow routes liveness data to Unissey
     via WebSocket
de/idnow/ai/websocket/nfc/                <- ICAO 9303 ePassport NFC reading
de/idnow/ai/websocket/emiratesnfc/         <- UAE identity document NFC reading
```

No response was received naming this finding, including the direct question of whether Art. 28 data-processing agreements exist with each of the three vendors and whether Unissey is individually named as a recipient under Art. 13(1)(e). The code path de/idnow/ai/websocket/unissey/ confirms IDnow internally routes biometric liveness data to Unissey, a sub-processor relationship not named anywhere in Tipico's privacy documentation. Three separate Art. 9(2) legal bases are required, one per processor, and none is individually docu-

mented. FaceTec's processing constitutes a US transfer with no confirmed Art. 46 safeguard disclosed to users. An Art. 35(3)(b) DPIA is mandatory for processing of this scale and is not confirmed to exist.

Impact: Special-category biometric data is processed by three independent vendors, including an internal, undisclosed routing of liveness data from one processor to another, with no confirmed DPIA or complete Art. 9(2) legal basis documentation.

Fix: Name all three vendors individually as Art. 28 processors, disclose the IDnow-to-Unissey routing explicitly, publish the mandatory Art. 35(3)(b) DPIA, and confirm the Art. 46 transfer safeguard for FaceTec's US processing.

H1: FinTecSystems XS2A Wizard: direct PSD2 bank-account access, undisclosed processor

---

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

376 FinTecSystems AG (Munich) classes provide direct PSD2 payment-initiation and account-information access, routing bank credentials, account balance, and transaction history through FinTecSystems infrastructure.

No response was received naming this finding. FinTecSystems is not named as a data processor in Tipico's privacy documentation.

Impact: Bank credentials and full account and transaction data are processed by an undisclosed PSD2 payment processor.

Fix: Name FinTecSystems AG as a data processor under Art. 13(1)(e) and confirm its PSD2 PISP/AISP compliance basis.

H2: IDnow NFC ePassport chip reading: immutable government-issued biometric data

---

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

Dedicated NFC readers for ICAO 9303 standard ePassports and UAE identity documents extract facial photograph and, for biometric passports, fingerprint data stored on the chip.

No response was received naming this finding, including the specific Art. 9(2) legal basis for extracting immutable government-issued biometric data from a passport chip.

Impact: Immutable, government-issued biometric data is extracted from identity document chips with no individually stated legal basis.

Fix: Publish the specific Art. 9(2) legal basis for NFC ePassport chip data extraction.

H3: SAP Emarsys geofencing activates at device boot, feeds a behavioral-prediction engine

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

RegisterGeofencesOnBootCompletedReceiver activates location geofencing at device boot, before the app is opened. A separate Emarsys Predict component builds betting-behavior prediction profiles.

No response was received naming this finding. SAP Emarsys is not disclosed as a data processor, and behavioral-prediction profiling potentially engaging Art. 22 automated decision-making is not disclosed as a distinct processing activity.

Impact: Location tracking begins before the app is opened, and a betting-behavior prediction engine operates with no disclosed Art. 22 assessment.

Fix: Disclose SAP Emarsys as a processor, restrict geofence registration to app-open sessions, and assess Emarsys Predict against Art. 22.

H4: LiveSwitch WebRTC with full-screen MediaProjection capture capability

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

MediaProjectionSource and NativeMediaProjectionSource classes use Android's MediaProjection API, capable of capturing the entire device screen, backed by FOREGROUND_SERVICE_MEDIA_PROJECTION.

No response was received naming this finding. The scope of data transmitted via LiveSwitch is not individually disclosed.

Impact: A full-screen capture capability, not limited to camera video, operates with no disclosed scope of what is transmitted or to whom.

Fix: Disclose the specific feature requiring full-screen MediaProjection capture and its data-transmission scope under Art. 13(1)(c).

H5: IMEI collection alongside all-files device access, no disclosed purpose

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

READ_PHONE_STATE collects IMEI, phone number, and SIM serial; MANAGE_ALL_FILES_ACCESS_PERMISSION grants read/write access to any file on the device.

No response was received naming this finding. No disclosed purpose exists for either permission in a sports-betting application's privacy documentation.

Impact: Device-level identifiers and unrestricted file-system access are held with no stated purpose, a significant data-minimization concern.

Fix: Remove both permissions unless a specific, currently active feature requires each individually, and disclose that purpose if retained.

H6: IBM Instana: undisclosed network metadata capture from biometric, banking, and betting transactions

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

146 IBM Instana classes collect network request timing, HTTP response metadata, and error rates in real time, including metadata from biometric KYC, XS2A banking requests, and betting transactions.

No response was received naming this finding. IBM Instana is not disclosed as a data processor.

Impact: Network metadata from the app's most sensitive transaction categories is captured by an undisclosed monitoring processor.

Fix: Name IBM Instana as a data processor under Art. 13(1)(e).

H7: Advertising-attribution identifiers on a biometric and banking platform

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

ACCESS_ADSERVICES_ATTRIBUTION and AD_ID are declared alongside the biometric and banking processing described above.

No response was received naming this finding. OS-level advertising attribution alongside facial-biometric and live-banking-credential processing creates a cross-domain identity profile of exceptional sensitivity, with no individually disclosed Art. 6(1) legal basis.

Impact: Advertising attribution operates on the same platform as biometric and banking data, creating a uniquely sensitive cross-domain identity profile.

Fix: Disclose the Art. 6(1) legal basis for advertising attribution specifically in the context of this platform's other sensitive processing.

Tipico’s Response, Recorded in Full

The only reply received across the entire correspondence, from presse@tipico.com on 16 July 2026, in full: ”Sehr geehrter Herr Kepp, Vielen Dank für Ihre Nachricht. Wir bestätigen den Erhalt der von Ihnen zur Verfügung gestellten Informationen. Mit freundlichen Grüßen, Tipico Unternehmenskommunikation.” This is a one-line receipt acknowledgment; it does not name, dispute, or engage with a single one of the nine findings. RFI-IRFOS’s reply the next day rejected the acknowledgment as insufficient and requested a concrete meeting date. No further reply of any kind was received across five subsequent written notices and 65 further days through the close of the embargo.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1)(b), Art. 25(1)	Hardcoded, publicly extractable production credentials, 11 modules
C2	GDPR Art. 9(2), Art. 13(1)(e), Art. 44-49	Undisclosed inter-vendor biometric sub-processor chain
H1	GDPR Art. 13(1)(e); PSD2 Art. 66-67	Undisclosed PSD2 payment processor
H2	GDPR Art. 9(2), Art. 13(1)(c)	Immutable biometric data from passport chips, no stated legal basis
H3	GDPR Art. 5(1)(c), Art. 13(1)(e), Art. 22	Boot-time geofencing feeding undisclosed prediction engine
H4	GDPR Art. 5(1)(c), Art. 13(1)(c)	Undisclosed full-screen capture scope
H5	GDPR Art. 5(1)(c), Art. 13(1)(c)	Undisclosed IMEI and all-files access
H6	GDPR Art. 13(1)(e)	Undisclosed monitoring processor on sensitive transactions
H7	GDPR Art. 6(1), Art. 5(1)(c)	Advertising attribution on a biometric/banking platform

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent; internal-only relay address bounces; 9 findings
2026-06-28	Delivery-fix resend to compliance@tipico.com succeeds
2026-07-16	Only reply received: a one-line receipt acknowledgment from presse@tipico.com, naming no finding
2026-07-17	RFI-IRFOS rejects the acknowledgment as insufficient, requests a concrete meeting date
2026-07-27 / 08-04 / 08-15 / 09-04	Follow-ups restate all nine findings; Malta's IDPC added to cc from 08-15
2026-09-12	Final follow-up, 83 days since disclosure, restates full findings, weekly SHA-256 re-diffing confirmed
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Nine written notices across 91 days produced exactly one reply, a one-line acknowledgment addressing none of the nine findings. All nine findings, including an undisclosed sub-processor chain routing biometric liveness data between two independent vendors, stand exactly as originally reported.

Residual Risk & Recommendations

- Disclose the IDnow-to-Unissey biometric data routing explicitly and publish the mandatory Art. 35(3)(b) DPIA; this is the single highest-priority item given the scale and undisclosed nature of this cross-vendor data flow.
- Rotate the Firebase credential and audit security rules across all eleven active modules.
- Name FinTecSystems, SAP Emarsys, and IBM Instana individually as data processors.
- Disclose the full-screen capture scope of LiveSwitch and remove or justify IMEI and all-files access.
- Establish a substantive reply path independent of the press office, which produced only a one-line acknowledgment across 91 days.

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