



Coordinated Security & Privacy Disclosure, Final Report

win2day for Android (at.win2day.games, v2.15.1, versionCode 50518)

Ten written notices, ninety-one days, total silence – not one reply of any kind

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL SIX FINDINGS UNADDRESSED AFTER TEN NOTICES, ZERO REPLIES

Target	Casinos Austria / Oesterreichische Lotterien group
Product audited	win2day for Android, at.win2day.games, v2.15.1 (versionCode 50518), Austria's licensed real-money online casino app
Disclosure reference	REF WIN2DAY-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 undisclosed GlassBox/ClariSite session-replay SDK capturing every tap and form entry, including potentially masked payment fields, CVSS v4.0 8.7, unaddressed)

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	Findings	4
3.1	C1: GlassBox / ClariSite session-recording SDK – 801 classes active in the production APK	4
3.2	C2: Firebase production credentials hardcoded	5
3.3	H1: Salesforce Marketing Cloud – gambling behavioral CRM data sent to US infrastructure	5
3.4	H2: Network Security Config present but no certificate pinning	6
3.5	H3: ACCESS_ADSERVICES_ATTRIBUTION and AD_ID on a state-licensed gambling platform	6
3.6	H4: Usercentrics CMP deployed but GlassBox not listed as a processing activity	6
4	Ten Notices, Total Silence	7
5	Data Protection, Article by Article	7
6	Disclosure Timeline & Outcome	8
7	Residual Risk & Recommendations	8

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production win2day Android application, Austria's licensed real-money online casino platform, and identified two CRITICAL and four HIGH findings: a GlassBox/ClariSite session-recording SDK (801 combined small classes) active in the release build, capable of capturing every tap, screen state, and form entry, including potentially masked payment and banking fields, and not individually disclosed as a data processor in either win2day's privacy documentation or its Usercentrics consent-management platform, Firebase production credentials hardcoded in the shipped APK, a Salesforce Marketing Cloud integration (1,040 classes) sending gambling behavioral data, games played, session duration, deposit frequency, to US infrastructure with no individual disclosure, raising a potential conflict with responsible-gambling obligations for at-risk player re-engagement, a Network Security Configuration present but with no certificate pinning on a real-money financial gambling platform, an OS-level advertising attribution permission (ACCESS_AD SERVICES_ATTRIBUTION) creating a cross-platform gambling-behavior ad profile with no stated individual Art. 6(1) legal basis, and a deployed Usercentrics consent-management platform that does not list GlassBox/ClariSite session recording as a processing activity, giving users a false assurance of complete disclosure.

Across ten written notices over ninety-one days, cc'd or bcc'd throughout to the Austrian Datenschutzbehörde and CERT.at, no reply of any kind, human or automated, was ever received from win2day, CAL, Oesterreichische Lotterien, or Casinos Austria AG. presse@casinosaustriaag.com failed delivery repeatedly with DNS resolution errors in late June and was never confirmed reachable at any later point. Whether the Art. 33(4) 72-hour breach-notification argument raised on 24 August was ever acted upon internally, or escalated further by either regulator notified, is unknown, since no reply of any kind exists in this correspondence at all.

Scope: Static analysis of the publicly downloaded production win2day Android APK (v2.15.1), on an authorized test device, only. No win2day account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 20 June 2026 to datenschutz@cal.at, cc security@win2day.at, bcc the Austrian Datenschutzbehörde and CERT.at. Across ten written notices over ninety-one days, addressed variously to datenschutz@cal.at, help@win2day.at, office@lotterien.at, datenschutz@lotterien.at, and presse@casinosaustriaag.com (which failed delivery repeatedly with DNS errors), no reply of any kind was ever received from win2day, CAL, Oesterreichische Lotterien, or Casinos Austria AG.

ID	Severity	Title
C1	CRITICAL	GlassBox / ClariSite session-recording SDK – 801 classes active in the production APK
C2	CRITICAL	Firebase production credentials hardcoded
H1	HIGH	Salesforce Marketing Cloud – gambling behavioral CRM data sent to US infrastructure

ID	Severity	Title
H2	HIGH	Network Security Config present but no certificate pinning
H3	HIGH	ACCESS_AD SERVICES_ATTRIBUTION and AD_ID on a state-licensed gambling platform
H4	HIGH	Usercentrics CMP deployed but GlassBox not listed as a processing activity

Subject & Operator Analysis

win2day is operated by the Casinos Austria / Oesterreichische Lotterien group, Austria's licensed operator for real-money online casino and lottery gaming.

Findings

C1: GlassBox / ClariSite session-recording SDK – 801 classes active in the production APK

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/clarisite/mobile/ (762 smali classes) and com/glassbox/android/ (39 smali classes), 801 classes total, are active in the release build. This session-replay SDK is capable of capturing every tap, screen state, and form entry, including potentially masked payment and banking fields, on Austria's only licensed real-money online casino app. It is not individually disclosed as a data processor in win2day's privacy documentation or in its Usercentrics CMP.

No reply of any kind, across ten notices, addressed this finding.

Impact: Payment and banking field entries may be captured via screen-replay on a real-money gambling platform, with no matching disclosure to users of this specific processing.

Fix: Exclude payment and banking input fields from GlassBox/ClariSite capture entirely, and disclose the SDK individually in the privacy documentation and consent platform.

C2: Firebase production credentials hardcoded

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

google_api_key AlzaSyA2-8aRd0x_ZUmsWkcKQHGGDHQW-_60DaA, google_app_id 1:257086460122:android:637f54fd5456361d, firebase_database_url https://win2day-1267.firebaseio.com, project win2day-1267, all extractable from the public Play Store APK in under 60 seconds.

No reply of any kind addressed this finding.

Impact: A production Firebase project's attack surface, on a real-money gambling platform, cannot be independently ruled safe from outside the console once its key ships in every installed client.

Fix: Rotate the exposed key, confirm deny-by-default security rules, and enforce App Check for this project.

H1: Salesforce Marketing Cloud – gambling behavioral CRM data sent to US 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

1,040 smali classes implement Salesforce Marketing Cloud, receiving gambling behavioral data, games played, session duration, deposit frequency, on US infrastructure; not individually disclosed.

This raises a potential conflict with responsible-gambling obligations if the same behavioral profile used for regulatory duty-of-care purposes is also used for at-risk player re-engagement marketing. No reply of any kind addressed this finding.

Impact: Gambling behavioral data may be used for marketing re-engagement of the same players a responsible-gambling framework is meant to protect, with no individual disclosure of this specific processor.

Fix: Disclose Salesforce Marketing Cloud individually as a processor and confirm behavioral data used for responsible-gambling duty-of-care is segregated from marketing re-engagement use.

H2: Network Security Config present but no certificate pinning

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

A Network Security Config exists but relies on system CA trust only; any certificate authority in the device's root trust store can issue an accepted certificate on a real-money financial gambling platform.

No reply of any kind addressed this finding.

Impact: Financial transaction traffic on a real-money gambling platform can be intercepted or altered by any party able to install a trusted certificate on the network path.

Fix: Implement certificate pinning for all win2day financial and account endpoints.

H3: ACCESS_ADSERVICES_ATTRIBUTION and AD_ID on a state-licensed gambling platform

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

OS-level advertising-attribution permissions are declared, creating a cross-platform gambling-behavior ad profile with no stated individual Art. 6(1) legal basis.

No reply of any kind addressed this finding.

Impact: A cross-platform advertising profile built from gambling-behavior data may be constructed with no confirmed individual lawful basis for that specific processing.

Fix: Deploy a consent-management gate specific to advertising-attribution collection, with a stated Art. 6(1) legal basis.

H4: Usercentrics CMP deployed but GlassBox not listed as a processing activity

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 Usercentrics CMP (1,545 classes) is active, but GlassBox/ClariSite session recording (C1) is not individually disclosed or consentable within it.

This gives users a false assurance that the consent platform covers all data processing occurring in the app, when a significant session-replay capability sits outside its scope entirely. No reply of any kind addressed this finding.

Impact: Users relying on the visible consent platform to understand what is collected are given an incomplete picture, since a major capture mechanism is not represented there at all.

Fix: Add GlassBox/ClariSite as an explicit, individually consentable processing activity within the Usercentrics CMP.

Ten Notices, Total Silence

Across ten written notices over ninety-one days, addressed to five different mailboxes across the Casinos Austria / Oesterreichische Lotterien group, no reply of any kind, human or automated, was ever received. presse@casinosaustriaag.com failed delivery repeatedly with DNS resolution errors and was never confirmed reachable at any later point in the correspondence.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 13(1)(e)(f)	Undisclosed session-replay capture of potentially payment-adjacent screen data
C2	GDPR Art. 25(1), Art. 32(1)(b)	Hardcoded Firebase credentials on a real-money gambling platform
H1	GDPR Art. 13(1)(e), Art. 46	Undisclosed gambling-behavior CRM transfer to US infrastructure
H2	GDPR Art. 32(1)(a)	No certificate pinning on financial gambling transaction traffic
H3	GDPR Art. 6(1)	Cross-platform ad-attribution profile with no stated legal basis
H4	GDPR Art. 13, Art. 7	Consent platform omitting a major processing activity

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to datenschutz@cal.at, cc security@win2day.at, bcc Austrian DSB/CERT.at; 2 CRITICAL + 4 HIGH findings
2026-06-27	Follow-up widens recipients to help@win2day.at, office@lotterien.at, datenschutz@lotterien.at, presse@casinosaustriaag.com (fails delivery repeatedly)
2026-08-24	Follow-up, sixty-five days, 'not a single human,' invokes the Art. 33(4) 72-hour notification clock
2026-09-04	Follow-up, fifteen days until embargo, REF at.win2day.games stated explicitly
2026-09-16	Follow-up, deadline reached, three days before disclosure
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Establish a functioning response process across the group's datenschutz@ mailboxes.
- Exclude payment and banking fields from GlassBox/ClariSite session-replay capture and disclose the SDK individually.
- Implement certificate pinning for all financial and account endpoints.
- Rotate the exposed Firebase key.
- Add GlassBox/ClariSite as an explicit processing activity within the Usercentrics CMP.

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. GDPR Art. 6, 7, 13, 25, 32, 46. REF WIN2DAY-2026-R1.