



---

# Security & Privacy Disclosure, Final Report

**bwin Austria Games for Android ([at.equadrat.bwinaustria.games](mailto:at.equadrat.bwinaustria.games))**

An unlicensed real-money online casino operating in Austria without a GSpG license, no functional age-assurance for gambling access, and six further undisclosed data flows, including affiliate device tracking and in-casino GPS access, unresolved through 119 days and a 28-day-overdue embargo, with zero substantive reply from any of four directly-addressed Entain/bwin mailboxes

**PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 19 SEPTEMBER 2026, SEVEN FINDINGS REMAIN UNADDRESSED**

---

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Target</b>                    | Entain Group plc (bwin brand) · Developer: Equadrat Medien GmbH, Vienna, Austria                                                                                                                                                                                                                                                                                                                                       |
| <b>Package</b>                   | at.equadrat.bwinaustria.games                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Platform Audited</b>          | Android · v0.2.8 (versionCode 28), Flutter, static analysis of the production APK                                                                                                                                                                                                                                                                                                                                      |
| <b>Initial Disclosure (R1)</b>   | 2026-06-20                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Disclosure / Embargo Date</b> | 2026-09-19                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Report Published</b>          | 2026-10-17                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Overall Severity</b>          | CRITICAL                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Findings</b>                  | 7 (1 Critical, 6 High)                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Correspondence</b>            | 6 messages sent by RFI-IRFOS across two email threads to dataprotectionofficer@entaingroup.com, compliance@entainpartners.com, privacy@bwin.de, and amlreports@entaingroup.com (one send bounced: press@entaingroup.com), 7 automated non-substantive responses received (6 ticket-acknowledgment bots plus 1 automated reply redirecting data-subject-access requests elsewhere), 0 substantive replies ever received |
| <b>Authorities CC'd</b>          | Oesterreichische Datenschutzbehoerde (DSB)                                                                                                                                                                                                                                                                                                                                                                             |

---

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

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

## Contents

---

|           |                                                                                                               |           |
|-----------|---------------------------------------------------------------------------------------------------------------|-----------|
| <b>1</b>  | <b>Executive Summary</b>                                                                                      | <b>4</b>  |
| <b>2</b>  | <b>Subject &amp; Operator Context</b>                                                                         | <b>5</b>  |
| <b>3</b>  | <b>Engagement Summary</b>                                                                                     | <b>5</b>  |
| <b>4</b>  | <b>Findings</b>                                                                                               | <b>6</b>  |
| 4.1       | C1: Online casino operation in Austria without a GSpG license, no effective age gate . . . . .                | 6         |
| 4.2       | H1: Device-linked identifier transmitted to Entain's own affiliate network without disclosure . . . . .       | 7         |
| 4.3       | H2: localdetector.com: undisclosed third-party geolocation service used for jurisdiction checks . . . . .     | 7         |
| 4.4       | H3: Entire betting and casino data flow routed through an undisclosed foreign sports-data processor . . . . . | 8         |
| 4.5       | H4: Casino WebView requests GPS precision location with no disclosed purpose . . . . .                        | 8         |
| 4.6       | H5: Internal developer build path leaked in the production binary . . . . .                                   | 9         |
| 4.7       | H6: minSdk 24 (Android 7.0, 2016): real-money transactions on a decade-unpatched platform . . . . .           | 9         |
| <b>5</b>  | <b>Impact Analysis</b>                                                                                        | <b>10</b> |
| <b>6</b>  | <b>The Complete Chain: Six Messages, Four Mailboxes, Zero Human Replies, 119 Days</b>                         | <b>10</b> |
| <b>7</b>  | <b>Data Protection — Article by Article</b>                                                                   | <b>11</b> |
| <b>8</b>  | <b>Regulatory &amp; Legal Landscape</b>                                                                       | <b>11</b> |
| <b>9</b>  | <b>Indicators of Compromise</b>                                                                               | <b>12</b> |
| <b>10</b> | <b>Disclosure Timeline &amp; Outcome</b>                                                                      | <b>13</b> |
| <b>11</b> | <b>Residual Risk &amp; Recommendations</b>                                                                    | <b>13</b> |

## Executive Summary

bwin Austria Games (at.equadrat.bwinaustria.games) is Entain Group plc's Austrian-market real-money gambling app, developed by Equadrat Medien GmbH (Vienna) and distributed under the bwin brand, offering sports betting and online casino games with real financial deposits and withdrawals. Static analysis of the production APK (v0.2.8) found this app to have a cleaner security baseline than most of the 30 apps in RFI-IRFOS's current research series: it is the first app in that series to not hardcode a Firebase production key, it ships a near-minimal permission set, and it builds against a current compileSdk. None of that changes the finding that opens this report.

RFI-IRFOS identified 1 CRITICAL and 6 HIGH severity findings. The app actively delivers online casino games (slots, table games) to Austrian users without holding an Austrian Glueck-spielgesetz (GSpG) license, a form of gambling operation that Austrian law reserves exclusively for Casinos Austria AG (win2day); no age-verification logic, flow, or strings were identified anywhere in the production binary (C1). Six further findings are HIGH: a device-linked identifier transmitted to Entain's own affiliate marketing network without disclosure (H1), an undisclosed third-party geolocation service used for jurisdiction checks (H2), the app's entire betting and casino data flow routed through an undisclosed foreign sports-data processor (H3), a casino WebView that separately requests GPS precision location despite IP-based geolocation already being in use (H4), an internal developer build path leaked in the production binary that confirms the mobile app and backend share a repository (H5), and a minimum supported Android version (24, 2016) that permits real-money financial transactions on roughly a decade of unpatched devices (H6).

RFI-IRFOS disclosed these findings on 20 June 2026 to dataprotectionofficer@entaingroup.com, CC legal@bwin.com. Five further messages followed over the next 72 days, broadening the recipient list to compliance@entainpartners.com, privacy@bwin.de, and amlreports@entaingroup.com, and adding the Austrian Datenschutzbehoerde to CC from the third message onward. One CC address, press@entaingroup.com, bounced outright. Across the full record, the only inbound activity on any of these addresses was six generic, single-use ticket-acknowledgment bots and one automated reply from the DPO address itself instructing senders to route data-subject-access and deletion requests elsewhere, a message that did not engage with either the unlicensed-operation finding or any of the six GDPR findings. No human reply was ever received from dataprotectionofficer@entaingroup.com, compliance@entainpartners.com, privacy@bwin.de, or amlreports@entaingroup.com. The stated embargo of 19 September 2026 passed 28 days before this report's publication date, with all seven findings unaddressed.

| ID | Severity        | Title                                                                                           |
|----|-----------------|-------------------------------------------------------------------------------------------------|
| C1 | <b>CRITICAL</b> | Online casino operation in Austria without a GSpG license, no effective age gate                |
| H1 | <b>HIGH</b>     | Device-linked identifier transmitted to Entain's own affiliate network without disclosure       |
| H2 | <b>HIGH</b>     | localdetector.com: undisclosed third-party geolocation service used for jurisdiction checks     |
| H3 | <b>HIGH</b>     | Entire betting and casino data flow routed through an undisclosed foreign sports-data processor |

| ID | Severity | Title                                                                                 |
|----|----------|---------------------------------------------------------------------------------------|
| H4 | HIGH     | Casino WebView requests GPS precision location with no disclosed purpose              |
| H5 | HIGH     | Internal developer build path leaked in the production binary                         |
| H6 | HIGH     | minSdk 24 (Android 7.0, 2016): real-money transactions on a decade-unpatched platform |

## Subject & Operator Context

bwin Austria Games is operated under license from Entain Group plc, a London Stock Exchange-listed gambling group, and developed by Equadrat Medien GmbH in Vienna. The app processes real-money deposits, withdrawal requests, live sports-betting stakes, and casino-game wagers for Austrian users.

As with several apps in this research series, the general engineering baseline here is better than average: no hardcoded Firebase credentials (the first app in a 30-app series to get this right), a minimal declared permission set, and a current compileSdk. That makes the central finding of this report more notable, not less: a categorical legal violation does not require sloppy engineering to exist alongside it. bwin Austria Games delivers online casino games to Austrian users without the single license Austrian law requires for that activity, and ships no functional age-assurance mechanism for a product that accepts real financial deposits.

## Engagement Summary

RFI-IRFOS sent the initial disclosure on 20 June 2026 to [dataprotectionofficer@entaingroup.com](mailto:dataprotectionofficer@entaingroup.com), [CC.legal@bwin.com](mailto:CC.legal@bwin.com), setting an embargo date of 19 September 2026. The only same-day response was an automated reply from the DPO address itself, stating that data-subject-access and deletion requests should be sent to a different, app-specific address, a message that did not acknowledge the security content of the disclosure at all.

A follow-up on 27 June 2026 broadened the recipient list to [privacy@bwin.de](mailto:privacy@bwin.de), [compliance@entaingroup.com](mailto:compliance@entaingroup.com), and [amlreports@entaingroup.com](mailto:amlreports@entaingroup.com), [CC.legal@bwin.com](mailto:CC.legal@bwin.com), [press@entaingroup.com](mailto:press@entaingroup.com), and [investors@entaingroup.com](mailto:investors@entaingroup.com). The [press@entaingroup.com](mailto:press@entaingroup.com) address bounced outright (mailer-daemon, address not found). From 23 July 2026 onward, RFI-IRFOS narrowed the direct recipients to [dataprotectionofficer@entaingroup.com](mailto:dataprotectionofficer@entaingroup.com) and [compliance@entaingroup.com](mailto:compliance@entaingroup.com), [CC.legal@bwin.com](mailto:CC.privacy@bwin.de) and, from this message forward, the Austrian Datenschutzbehörde. Further follow-ups were sent on 5 August (46 days after the original disclosure), 15 August (56 days), and 31 August 2026 (72 days, 16 days after the prior message), each restating the three open questions: whether bwin holds an Austrian GSpG license for the casino games it delivers, whether a documented remediation plan exists for the one Critical and six High findings, and whether these would be addressed before or after a regulator became involved.

Across this entire record, spanning four directly-addressed mailboxes and six messages, the only inbound activity was six separate, single-message ticket-acknowledgment bots ([compliance@entaingroup.com](mailto:compliance@entaingroup.com) and, once, [privacy@bwin.de](mailto:privacy@bwin.de), each generating a numbered support ticket such as #35425949 through #37045110) and the one automated DPO redirect on day one. No named human at Entain or bwin ever replied to any of the three questions, and

no reply of any kind addressed the GSpG license question or the unlicensed-casino finding specifically. The stated embargo of 19 September 2026 passed 28 days before this report's publication, with the correspondence record unchanged since 31 August.

## Findings

### C1: Online casino operation in Austria without a GSpG license, no effective age gate

**CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N, 2.1) — a categorical, unlicensed real-money gambling operation with no functional age assurance, blast-radius escalated from LOW**

```
https://api-v2.sb-scores.com/Casino/Games?&app_id=22
assets/flutter_assets/assets/images/Casino.png
```

Austrian GSpG Section 14: online casino operation reserved exclusively  
for Casinos Austria AG (win2day.at)

Age verification logic, strings, or flow: NONE identified

Enforcement jurisdiction: Austrian Finanzpolizei (BMF); EU DSA Art. 28  
age-assurance obligation falls under BMDW jurisdiction

**Impact:** RFI-IRFOS blast-radius escalation: raised from LOW/2.1 to CRITICAL because Austrian federal law (Glueckspielgesetz, GSpG Section 14) reserves online casino operation exclusively for Casinos Austria AG (win2day); no private operator, including Entain plc, currently holds a valid Austrian online casino license. The production APK confirms active casino game delivery to Austrian users via `api-v2.sb-scores.com/Casino/Games`, and no age-verification logic, strings, or flow were identified anywhere in the production binary. This is a categorical legal violation, not a grey area: Austrian courts have established that contracts for casino games with unlicensed operators are void under Section 879 ABGB, players may recover losses, and GSpG Section 52 provides for administrative penalties. Combined with the complete absence of age assurance on a real-money product, the blast radius here is regulatory enforcement exposure and direct access by minors to real-money gambling, neither of which a technical CVSS vector captures on its own.

## H1: Device-linked identifier transmitted to Entain's own affiliate network without disclosure

**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)**  
**— undisclosed cross-device affiliate attribution on a real-money financial app, blast-radius escalated from MEDIUM**

```
_initializeApp: deviceId = '...' (initialization log)
loadDeviceId / setDeviceId (device ID management functions)

https://mediaserver.entainpartners.com/renderBanner.do
?zoneId=2123556
&tdpeh=Screen-Scores_Placement-B0TD__$GUID_device-$DeviceHashedId
&btag=301645
```

**Impact:** RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.1 to HIGH because the production Dart binary generates a device identifier and transmits it, along with an affiliate tracking tag (btag=301645), to mediaserver.entainpartners.com, Entain's own affiliate/partner marketing network, on a real-money financial application. This cross-device affiliate attribution is not disclosed as a processing activity in the available privacy documentation. Combining undisclosed device-level tracking with a product that processes gambling deposits and withdrawals raises the practical stakes beyond a typical undisclosed-SDK finding.

## H2: localdetector.com: undisclosed third-party geolocation service used for jurisdiction checks

**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, 4.5)**  
**— undisclosed third party performs the jurisdiction check that gates real-money gambling access, blast-radius escalated from MEDIUM**

```
https://api.localdetector.com/Data/Init/LocalData/
(called on startup via fetchLocalDataFromNetwork)

Not named as a data processor or recipient in available privacy
documentation
```

**Impact:** RFI-IRFOS blast-radius escalation: raised from MEDIUM/4.5 to HIGH because the app calls api.localdetector.com/Data/Init/LocalData/ on startup via fetchLocalDataFromNetwork, an undisclosed third-party geolocation/locale detection service not named as a data processor or recipient in any available privacy documentation. For a gambling operator, geolocation determines whether a user is in a jurisdiction permitted to gamble at all; outsourcing that determination to an undisclosed third party raises the stakes of this finding above a typical undisclosed-SDK case.

### H3: Entire betting and casino data flow routed through an undisclosed foreign sports-data processor

**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, 4.8) — all betting behaviour flows through an undisclosed Israel-based processor with no documented Art. 44 safeguard, blast-radius escalated from MEDIUM**

```
https://api-v2.sb-scores.com/      (core API, internal project
                                   name: sb-scores-app-new)
https://imagescache.365scores.com/ (sports imagery CDN)
https://mobilews.365scores.com/    (live scores / bets of the day)

365scores / SportsDataIO (Israel): not named as a data processor or
international transfer recipient in available privacy documentation
```

**Impact:** RFI-IRFOS blast-radius escalation: raised from MEDIUM/4.8 to HIGH because the app's entire betting and casino infrastructure routes through api-v2.sb-scores.com, imagescache.365scores.com, and mobilews.365scores.com. 365scores (now part of SportsDataIO, headquartered in Israel) provides the live scores, match data, and odds infrastructure behind every bet placed. Neither sb-scores.com nor 365scores.com is named as a data processor or international transfer recipient in the available privacy documentation. Israel has an EU adequacy decision, but the transfer relationship and data scope remain undisclosed, and this is the processor behind every betting interaction in the app, not a peripheral feature.

### H4: Casino WebView requests GPS precision location with no disclosed purpose

**HIGH (CVSS v4.0 AV:N/AC:L/AT:N/PR:L/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.3) — precise-location collection inside casino content duplicates an already-undisclosed jurisdiction check, blast-radius escalated from MEDIUM**

```
webview_flutter_android, casino game content:
  onGeolocationPermissionsShowPrompt
  onGeolocationPermissionsHidePrompt
  GeolocationPermissionsCallback

Jurisdiction check already performed via IP geolocation (see H2);
no disclosed purpose for additional GPS precision
```

**Impact:** RFI-IRFOS blast-radius escalation: raised from MEDIUM/4.3 to HIGH because casino game content loaded inside the app's WebView (webview\_flutter\_android) triggers Android's WebView geolocation permission API (onGeolocationPermissionsShowPrompt, onGeolocationPermissionsHidePrompt, GeolocationPermissionsCallback), requesting GPS precision location at runtime. IP-based jurisdiction checking is already performed via localdetector.com (H2); casino game content has no disclosed legitimate purpose requiring GPS precision on top of that, and any GPS data collected during casino sessions flows to third-party game providers without disclosure.

## H5: Internal developer build path leaked in the production binary

**HIGH (CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N, 3.1)**  
 — confirms shared repo structure between the mobile app and the financial backend, blast-radius escalated from LOW

```
file:///Users/yifat/AndroidStudioProjects/sb-scores-app-new/client/
    .dart_tool/flutter_build/dart_plugin_registrant.dart
```

Exposes: developer first name, internal project name  
 (sb-scores-app-new), shared repo between app and backend API

**Impact:** RFI-IRFOS blast-radius escalation: raised from LOW/3.1 to HIGH because the Flutter Dart runtime binary (libapp.so) contains a full developer build path (file:///Users/yifat/AndroidStudioProjects/sb-scores-app-new/client/.dart\_tool/flutter\_build/dart\_plugin\_registrant.dart), exposing the developer's first name, the internal project name (sb-scores-app-new), and confirmation that the mobile app and the backend API share a single repository. On a financial, real-money application, this kind of internal-structure leakage aids targeted reconnaissance against the backend infrastructure that processes gambling deposits and withdrawals, which is a materially different risk than the same leak on a non-financial app.

## H6: minSdk 24 (Android 7.0, 2016): real-money transactions on a decade-unpatched platform

**HIGH (CVSS v4.0 AV:P/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 4.0)**  
 — financial deposits and withdrawals permitted on roughly ten years of unpatched Android versions, blast-radius escalated from MEDIUM

```
minSdk 24 (Android 7.0 Nougat, released 2016, ~10 years unpatched)
compileSdk / targetSdk 36 (current)
```

Real-money transaction types permitted on minSdk 24: deposits,  
 withdrawals, live betting stakes, casino wagers

**Impact:** RFI-IRFOS blast-radius escalation: raised from MEDIUM/4.0 to HIGH because minSdk 24 permits real-money gambling transactions, deposits, withdrawals, and live betting stakes, on Android 7.0 Nougat devices from 2016 that have not received security patches for approximately a decade. For a financial application processing gambling deposits and withdrawals, this does not meet the standard of technical measures proportionate to financial risk that GDPR Art. 32(1)(a) requires.

## Impact Analysis

---

bwin Austria Games is an unusual case in this disclosure series in the same way Zalando was: the general engineering baseline is better than average (no hardcoded Firebase key, minimal permissions, current compileSdk), which makes the central finding more notable, not less. C1 is not a technical bug that better engineering practice would have prevented; it is the operation of a regulated real-money product in a market where the operator does not hold the single license that market requires, combined with the complete absence of age assurance for that same product. The six HIGH findings share a common shape with other apps in this series: real, functioning data flows (affiliate device tracking, jurisdiction geolocation, sports-data infrastructure, in-casino GPS access) that are not disclosed to users in a way that satisfies GDPR Art. 13's transparency requirement, on a product where the underlying activity is already unlicensed.

The correspondence failure compounds this. Four separate Entain/bwin mailboxes were directly addressed, [dataprotectionofficer@entaingroup.com](mailto:dataprotectionofficer@entaingroup.com), [compliance@entainpartners.com](mailto:compliance@entainpartners.com), [privacy@bwin.de](mailto:privacy@bwin.de), and [amlreports@entaingroup.com](mailto:amlreports@entaingroup.com), and not one of them produced a human reply across 72 days and six messages. The only response from the DPO address itself was an automated message redirecting data-subject-access requests elsewhere, which did not engage with either the license question or the six GDPR findings.

### The Complete Chain: Six Messages, Four Mailboxes, Zero Human Replies, 119 Days

---

Step 1, Disclosure sent: RFI-IRFOS sends the original 1 Critical / 6 High findings to [dataprotectionofficer@entaingroup.com](mailto:dataprotectionofficer@entaingroup.com) on 20 June 2026, CC [legal@bwin.com](mailto:legal@bwin.com), stating a 19 September 2026 embargo. The same-day response is an automated reply from the DPO address instructing senders to use a different address for data-subject-access and deletion requests, unconnected to the disclosure's actual content.

Step 2, Broadened recipients, a bounce: On 27 June 2026, RFI-IRFOS adds [privacy@bwin.de](mailto:privacy@bwin.de), [compliance@entainpartners.com](mailto:compliance@entainpartners.com), and [amlreports@entaingroup.com](mailto:amlreports@entaingroup.com) as direct recipients, CC [legal@bwin.com](mailto:legal@bwin.com), [press@entaingroup.com](mailto:press@entaingroup.com), and [investors@entaingroup.com](mailto:investors@entaingroup.com). [press@entaingroup.com](mailto:press@entaingroup.com) bounces outright.

Step 3, The Austrian DSB joins CC: On 23 July 2026, 27 days with no substantive reply, RFI-IRFOS follows up to [dataprotectionofficer@entaingroup.com](mailto:dataprotectionofficer@entaingroup.com) and [compliance@entainpartners.com](mailto:compliance@entainpartners.com), now CC'ing [privacy@bwin.de](mailto:privacy@bwin.de) and the Austrian Datenschutzbehörde for the first time. The only inbound activity remains generic ticket-acknowledgment bots, one per message.

Step 4, 46 and 56 days: Follow-ups on 5 August and 15 August 2026 restate the three open questions (GSpG license status, remediation plan, timing relative to regulator involvement). Each produces exactly one more numbered ticket-acknowledgment bot and no human reply.

Step 5, 72 days, last message: On 31 August 2026, RFI-IRFOS sends a final follow-up noting 16 days since the prior message and 72 days since the original disclosure, restating the same three questions verbatim. No reply of any kind follows this message through the embargo date.

Step 6, Embargo reached, then passed: The stated embargo of 19 September 2026 passes with the correspondence record unchanged: six RFI-IRFOS messages, one bounce, seven automated non-substantive responses (six ticket bots plus the day-one DPO redirect), zero

human replies, zero engagement with the license question.

Step 7, Publication: This report publishes 28 days after the embargo date, on the terms stated from the first message.

Across 119 days and four directly-addressed mailboxes at a London Stock Exchange-listed gambling group, not one produced a human reply to a disclosure naming an unlicensed real-money casino operation and an absent age gate.

## Data Protection — Article by Article

---

Art. 6(1)(b) GDPR, lawfulness of processing: C1's unlicensed casino operation undermines the lawful basis for any casino-related data processing that depends on a valid contract, since Austrian courts treat contracts for casino games with unlicensed operators as void.

Art. 13(1)(e) GDPR, recipients of personal data: H1's affiliate device-ID transmission to entain-partners.com, H2's localdetector.com geolocation call, and H3's 365scores/sb-scores data flow are all undisclosed recipients that Art. 13 requires to be named.

Art. 5(1)(c) GDPR, data minimisation: H4's GPS precision-location request inside casino content duplicates a jurisdiction check already performed via IP geolocation, collecting more than is necessary for the stated purpose.

Art. 25(1) GDPR, data protection by design: H5's leaked developer build path is a release-hardening failure inconsistent with privacy and security by design.

Art. 32(1)(a) GDPR, security of processing: H6's minSdk 24 permits real-money financial transactions on roughly a decade of unpatched Android versions, short of the proportionate technical measures Art. 32 requires for financial risk of this kind.

## Regulatory & Legal Landscape

---

bwin Austria Games is operated by Entain Group plc (London Stock Exchange-listed) under the bwin brand; bwin Interactive Entertainment AG was historically headquartered in Vienna, and the Austrian Datenschutzbehörde was CC'd on this disclosure from the third message onward. The GSpG finding (C1) sits within the jurisdiction of the Austrian Finanzpolizei (Bundesministerium fuer Finanzen); the EU Digital Services Act Art. 28 age-assurance obligation falls under BMDW jurisdiction for Austrian-market platforms.

Fine exposure under GDPR: Art. 83(5) applies to the Art. 6 lawfulness issue in C1 and the Art. 13 transparency issues in H1 through H3, up to EUR 20,000,000 or 4% of total worldwide annual turnover. Art. 83(4) applies to the Art. 32 security-of-processing issue in H6, up to EUR 10,000,000 or 2% of total worldwide annual turnover. Separately and outside GDPR entirely, GSpG Section 52 provides for administrative penalties against unlicensed gambling operators, and Austrian court precedent allows players to recover losses from contracts with unlicensed operators under Section 879 ABGB. That four directly-addressed Entain/bwin mailboxes, with the Austrian DSB in CC for the majority of the correspondence, produced zero human replies across 72 days is itself a fact relevant to any regulator assessing institutional engagement with a disclosed finding of this severity.

## Indicators of Compromise

---

The following endpoints, permissions, and paths were extracted from the production APK (v0.2.8, versionCode 28) via static analysis only. No bwin or Entain servers, accounts, or infrastructure were probed, and no account was created.

```
C1 -- api-v2.sb-scores.com/Casino/Games?&app_id=22, no age-gate  
    logic identified
```

```
H1 -- mediaserver.entainpartners.com/renderBanner.do,  
    $GUID_device + $DeviceHashedId + btag=301645
```

```
H2 -- api.localdetector.com/Data/Init/LocalData/
```

```
H3 -- api-v2.sb-scores.com, imagescache.365scores.com,  
    mobilews.365scores.com (365scores / SportsDataIO, Israel)
```

```
H4 -- webview_flutter_android, onGeolocationPermissionsShowPrompt  
    in casino WebView content
```

```
H5 -- file:///Users/yifat/AndroidStudioProjects/sb-scores-app-new/  
    client/.dart_tool/flutter_build/dart_plugin_registrant.dart
```

```
H6 -- minSdk 24 (Android 7.0 Nougat, 2016)
```

## Disclosure Timeline & Outcome

---

2026-06-20 Initial disclosure sent to dataprotectionofficer@entaingroup.com, CC legal@bwin.com. Automated DPO reply received same day, redirecting data-subject-access requests elsewhere, no substantive engagement.

2026-06-27 Follow-up sent to dataprotectionofficer@entaingroup.com, privacy@bwin.de, compliance@entainpartners.com, amlreports@entaingroup.com, CC legal@bwin.com, press@entaingroup.com, investors@entaingroup.com. press@entaingroup.com bounces. Ticket-acknowledgment bot received.

2026-07-23 Follow-up (27 days since original disclosure) to dataprotectionofficer@entaingroup.com and compliance@entainpartners.com, CC privacy@bwin.de and, for the first time, the Austrian Datenschutzbehoerde. Ticket-acknowledgment bot received.

2026-08-05 Follow-up (46 days). Ticket-acknowledgment bot #36417310 received. No substantive reply.

2026-08-15 Follow-up (56 days). Ticket-acknowledgment bot #36675829 received. No substantive reply.

2026-08-31 Follow-up (72 days since original disclosure, 16 days since prior message), restating all three open questions verbatim. Ticket-acknowledgment bot #37045110 received. No substantive reply.

2026-09-19 Stated embargo date reached. Correspondence record: six RFI-IRFOS messages, one bounce, seven automated non-substantive responses, zero human replies.

2026-10-17 This report published, 28 days after the embargo date. All seven findings confirmed unaddressed on the basis of the correspondence record.

## Residual Risk & Recommendations

---

C1 – Immediate: Cease delivery of casino games to Austrian users until a valid GSpG license is obtained, or confirm and document an alternative lawful basis if one exists that was not identified during this static-analysis-only audit. Implement functional age-assurance for all gambling access, not a cosmetic checkbox.

H1 – Near-term: Disclose the affiliate device-ID transmission to entainpartners.com as a data-sharing recipient, with its legal basis, in the privacy notice.

H2 – Near-term: Name localdetector.com as a data processor or recipient, with the specific jurisdiction-determination purpose it serves.

H3 – Near-term: Name 365scores/sb-scores (SportsDataIO) as a data processor and international transfer recipient, with a documented Art. 44 safeguard.

H4 – Near-term: Remove the casino WebView's GPS permission request unless a specific, disclosed purpose requires precision location beyond the IP-based jurisdiction check already in place.

H5 – Near-term: Strip developer build paths from release binaries as a standard release-hardening step.

H6 – Near-term: Evaluate raising minSdk for a financial application processing real-money gambling transactions.

Across all findings: establish a monitored path for security and data-protection disclosures that does not depend on four separate mailboxes producing nothing but ticket-acknowledgment bots. Over 72 days and six messages, not one of [dataprotectionofficer@entaingroup.com](mailto:dataprotectionofficer@entaingroup.com), [compliance@entainpartners.com](mailto:compliance@entainpartners.com), [privacy@bwin.de](mailto:privacy@bwin.de), or [amlreports@entaingroup.com](mailto:amlreports@entaingroup.com) produced a human reply to a disclosure naming an unlicensed real-money gambling operation, a finding that warrants review independent of the six GDPR findings in this report.

---

**RFI-IRFOS** [security@rfi-irfos.com](mailto:security@rfi-irfos.com) • [rfi-irfos.com](https://rfi-irfos.com)

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria All findings derive from static root-level analysis

of the published application using publicly available tooling. No bwin or Entain servers, accounts, or infrastructure were probed, and no account was created. Technical evidence is archived under chain of custody and will be provided to regulatory authorities on request. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF BWIN-2026.