



Security & Privacy Disclosure, Final Report

Österreichische Lotterien / Lotto for Android (at.lotterien.app)

Austria's state lottery operator instructs its entire user base to disable Android's core sideload protection to install the full app, hardcodes a production Firebase key, and runs a full Facebook Gaming Services integration plus every Privacy Sandbox advertising permission and fine-location collection on a state gambling platform, unresolved through 119 days and a 28-day-overdue embargo, with no substantive reply ever received

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

Target	Österreichische Lotterien GmbH, Rennweg 44, 1038 Vienna, Austria (≥90% state-owned)
Package	at.lotterien.app
Platform Audited	Android · v4.7.0 (versionCode 50983), static analysis of the production APK, 87.4MB
Initial Disclosure (R1)	2026-06-20 (REF LOTTO-2026)
Disclosure / Embargo Date	2026-09-19
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	7 (2 Critical, 5 High)
Correspondence	6 messages sent by RFI-IRFOS across two parallel email threads, 3 generic autoresponses received, 0 substantive replies from Österreichische Lotterien GmbH
Authorities BCC'd / CC'd	Austrian Datenschutzbehörde (DSB) · CERT.at · Österreichische Lotterien press office (presse@lotterien.at)

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

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

Contents

1	Executive Summary	4
2	Subject & Operator Context	5
3	Engagement Summary	5
4	Findings	6
4.1	C1: State lottery instructs users to disable Android sideload protection to install the full app, bypassing Play Protect	6
4.2	C2: Firebase production API key and project identifier hardcoded in the production binary	7
4.3	H1: Facebook SDK (1,234 classes incl. Gaming Services + production-present network debugger) processes lottery play data for Meta	7
4.4	H2: All four Android Privacy Sandbox advertising permissions declared simultaneously on a state gambling platform	8
4.5	H3: Precise GPS location (ACCESS_FINE_LOCATION) collected on a state lottery app with no documented purpose beyond jurisdictional checks	8
4.6	H4: Adjust (265 classes) + Adform (156 classes): dual, independent attribution SDKs on a state lottery	9
4.7	H5: Salesforce Marketing Cloud processes lottery behavioral data for US-based CRM re-engagement campaigns	9
5	Impact Analysis	10
6	The Complete Chain: Disclosure Across Two Threads, 119 Days, Zero Substantive Replies	10
7	Data Protection — Article by Article	11
8	Regulatory & Legal Landscape	11
9	Indicators of Compromise	12
10	Disclosure Timeline & Outcome	12
11	Residual Risk & Recommendations	13

Executive Summary

Österreichische Lotterien GmbH is Austria's state-owned lottery operator, ≥90% state-held, operating Lotto 6/45, EuroMillions, Brieflotterie, scratch tickets, and Glücksbörse for the entire Austrian adult population. Its Android application, `at.lotterien.app` (v4.7.0), was found during this audit to instruct its users to disable one of Android's core security protections in order to receive the app's full functionality — a decision made by a state entity, for a platform that handles active real-money gambling accounts, affecting a user base that includes elderly and technically inexperienced demographics disproportionately represented among lottery players.

Static analysis identified seven findings, two CRITICAL and five HIGH. The production update flow explicitly instructs users to enable 'install from unknown sources' because, per the app's own dialog text, Google's policies do not permit the full version to be distributed via the Play Store, bypassing Play Protect's security review and leaving the device's sideload protection permanently weakened afterward (C1). A Firebase production API key and project identifier are hardcoded in the APK, extractable in under 60 seconds (C2). A full Meta/Facebook SDK suite, 1,234 classes including Facebook Gaming Services and a production-present network debugging tool (Flipper), processes lottery play data on a state gambling platform (H1). All four Android Privacy Sandbox advertising permissions are declared simultaneously, an advertising-attribution stack layered onto state-run gambling (H2). Precise GPS location is collected with no disclosed purpose beyond what IP-based jurisdictional checks already provide (H3). Two independent attribution SDKs, Adjust (265 classes, Berlin) and Adform (156 classes, Copenhagen), both receive lottery-user behavioral data (H4). Salesforce Marketing Cloud processes detailed play-behavior data for CRM re-engagement campaigns on US infrastructure, a function in tension with the operator's own responsible-gambling obligations (H5).

RFI-IRFOS disclosed these findings on 20 June 2026 under REF LOTTO-2026 to `datenschutz@cal.at`, `CC help@lotterien.at`, BCC the Austrian DSB and CERT.at, restated in a follow-up on 27 June 2026 adding `presse@lotterien.at` to CC. A parallel escalation track was opened on 28 June 2026 directly to `help@lotterien.at` and `datenschutz@lotterien.at`, Lotterien's own customer-facing and data-protection addresses, after no substantive reply followed the first track, with further follow-ups on 5 August, 15 August, and 31 August 2026. Across both threads, six messages were sent in total. The only responses received, three in total, were a generic autoresponse template ('Vielen Dank für Ihre Anfrage... Aufgrund vieler Anfragen...') from `help@lotterien.at`, each arriving as an unthreaded, disconnected acknowledgment rather than a substantive reply. No acknowledgment, denial, or substantive reply was ever received from any named human at Österreichische Lotterien GmbH. The stated embargo of 19 September 2026 passed 28 days ago with all seven findings unaddressed.

ID	Severity	Title
C1	CRITICAL	State lottery instructs users to disable Android sideload protection to install the full app, bypassing Play Protect
C2	CRITICAL	Firebase production API key and project identifier hardcoded in the production binary
H1	HIGH	Facebook SDK (1,234 classes incl. Gaming Services + production-present network debugger) processes lottery play data for Meta

ID	Severity	Title
H2	HIGH	All four Android Privacy Sandbox advertising permissions declared simultaneously on a state gambling platform
H3	HIGH	Precise GPS location (ACCESS_FINE_LOCATION) collected on a state lottery app with no documented purpose beyond jurisdictional checks
H4	HIGH	Adjust (265 classes) + Adform (156 classes): dual, independent attribution SDKs on a state lottery
H5	HIGH	Salesforce Marketing Cloud processes lottery behavioral data for US-based CRM re-engagement campaigns

Subject & Operator Context

Österreichische Lotterien GmbH is Austria's state lottery operator, at least 90% state-owned, running Lotto 6/45, EuroMillions, Brieflotterie, scratch tickets, and the Glücksbörse secondary market for the entire adult Austrian population. Its Android app serves active real-money gambling accounts for a user base that, by the nature of a national lottery, skews toward demographics including elderly and technically inexperienced users who are disproportionately vulnerable to the specific risk created by Finding C1 below.

As a state entity, Österreichische Lotterien carries an elevated duty of care beyond what applies to a private commercial app. The findings in this report are not evidence of ordinary commercial SDK sprawl; several of them — the sideload instruction in particular — represent choices made by a government-owned operator that materially increase the security exposure of the Austrian public it serves.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 20 June 2026 under REF LOTTO-2026 to datenschutz@cal.at, CC help@lotterien.at, BCC the Austrian DSB and CERT.at. A follow-up was sent 27 June 2026 to the same thread, adding presse@lotterien.at to CC and restating the full finding set with the stated embargo date.

With no substantive reply to either message, RFI-IRFOS opened a second, parallel correspondence track on 28 June 2026 addressed directly to help@lotterien.at and datenschutz@lotterien.at, Österreichische Lotterien's own customer-facing and data-protection contact addresses, restating the disclosure and embargo date in full. Further follow-ups in this second thread were sent on 5 August, 15 August, and 31 August 2026, each restating the unresolved finding set and the approaching embargo. Across both threads, six messages were sent by RFI-IRFOS over the full correspondence period. The only responses received, three in total, arrived as a generic autoresponse template from help@lotterien.at ('Vielen Dank für Ihre Anfrage... Aufgrund vieler Anfragen bitten wir um etwas Geduld...'), each as its own disconnected, unthreaded acknowledgment rather than a substantive response addressing any of the seven findings. No named human at Österreichische Lotterien GmbH ever responded. The stated embargo of 19 September 2026 passed 28 days before this report's publication date.

Findings

C1: State lottery instructs users to disable Android sideload protection to install the full app, bypassing Play Protect

CRITICAL (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:A/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N, 7.3) — a state operator trains its entire user base, including elderly and technically inexperienced lottery players, to disable Android's core malware-sideload protection, blast-radius escalated from MEDIUM

"Aufgrund der restriktiven Richtlinien von Google kann die Vollversion der Lotterien App (inkl. Glücksbörse) nicht über den Google Play Store angeboten werden. Daher müssen Sie im Zuge der Aktualisierung, der Installation von „unbekannten Quellen“ zustimmen."

Effect: Play Protect scanning bypassed; "unknown sources" remains enabled after update; elevated phishing and MITM-sideload risk for the entire Austrian lottery user base.

Impact: RFI-IRFOS blast-radius escalation: raised from HIGH/7.3 to CRITICAL because the entity instructing users to disable Android's sideload protection is a state-owned lottery operator addressing the entire Austrian adult population, including elderly and technically inexperienced demographics who are disproportionately represented among lottery players and disproportionately vulnerable to the specific downstream risks this creates: a persistently weakened device setting after the update completes, trained trust in sideloaded installers that increases susceptibility to phishing, and a man-in-the-middle download vector with no Play Store integrity check to catch it. A private commercial app making this choice would already be a Art. 32/25 finding; a government-owned operator making the same choice for its entire user base is a materially larger blast radius.

C2: Firebase production API key and project identifier hardcoded in the production binary

CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.9) — unauthenticated backend reachable via a hardcoded key on a state gambling platform with active real-money accounts, blast-radius escalated from MEDIUM

```
res/values/strings.xml
google_api_key = AIzaSyDBPA6Fqixjq6RGP54GegQ1aqWfGuVmXDA
google_app_id = 1:938922098528:android:231774697466bc74
gcm_defaultSenderId = 938922098528
project_id = gluecksbote-c9560
firebase_database_url = https://gluecksbote-c9560.firebaseio.com
```

Impact: RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to CRITICAL because the key, its Firebase App ID, and its project identifier (gluecksbote-c9560) are extractable from the publicly distributed APK in under 60 seconds, and Österreichische Lotterien is a state-owned gambling operator with active real-money accounts, where the correctness of any Firebase security-rule restriction is self-administered and not independently verifiable from outside. For a state entity serving the entire Austrian population, the burden of demonstrating adequate restriction sits with the operator, not with the researcher who extracted the key.

H1: Facebook SDK (1,234 classes incl. Gaming Services + production-present network debugger) processes lottery play data for Meta

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) — a US third-country transfer of state lottery behavioral data via an undisclosed processor, with a debug network interceptor present in the production build

com/facebook/appevents/	App Events (behavioral analytics to Meta)
com/facebook/gamingservices/	Facebook Gaming Services
com/facebook/login/	Facebook Login
com/facebook/share/	Facebook Share
com/facebook/messenger/	Messenger SDK
com/facebook/flipper/	network debugger, present in production build
Total: 1,234 classes, Meta Platforms Inc. (US)	

Impact: The full Meta/Facebook SDK suite (1,234 smali classes) is present, including com/facebook/gamingservices (Facebook Gaming Services, an unusual integration for a state lottery platform) and com/facebook/flipper, a Facebook network-debugging tool typically restricted to development builds; its presence in the shipped production APK indicates it was not stripped from the release build process, and if active, every lottery API call transits through a Facebook debugging layer. Meta Platforms Inc. (US) receives behavioral analytics from a state gambling platform with no individually named processor agreement or Art. 44 transfer safeguard identified in the available privacy documentation.

H2: All four Android Privacy Sandbox advertising permissions declared simultaneously on a state gambling platform

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, 4.6)
— a full advertising-attribution and interest-profiling stack layered onto a state lottery, with potential responsible-gambling regulatory implications beyond GDPR

```
android.permission.ACCESS_AD SERVICES_TOPICS  
android.permission.ACCESS_AD SERVICES_CUSTOM_AUDIENCE  
android.permission.ACCESS_AD SERVICES_ATTRIBUTION  
android.permission.ACCESS_AD SERVICES_AD_ID  
com.google.android.gms.permission.AD_ID
```

Impact: All four Android Privacy Sandbox advertising permissions (Topics, Custom Audience, Attribution, Ad ID, plus the legacy AD_ID permission) are declared simultaneously, the full interest-profiling and behavioral-remarketing stack on a state-run lottery. No individual Art. 6(1) lawful basis is documented for each Privacy Sandbox data pipeline in the available privacy documentation. Beyond GDPR, advertising attribution and interest profiling of lottery players by the operator itself raises a question for the national gambling regulator on whether this is compatible with Österreichische Lotterien's own responsible-gambling obligations.

H3: Precise GPS location (ACCESS_FINE_LOCATION) collected on a state lottery app with no documented purpose beyond jurisdictional checks

HIGH (CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.0)
— GPS-precision location collected from lottery players where IP-based jurisdictional geolocation already suffices

```
android.permission.ACCESS_FINE_LOCATION  
android.permission.ACCESS_COARSE_LOCATION
```

Standard jurisdictional-check alternative: IP-based geolocation
(does not require device GPS precision)

Impact: ACCESS_FINE_LOCATION and ACCESS_COARSE_LOCATION are both declared. For an Austrian-only lottery, confirming a user is within jurisdiction is standard practice via IP-based geolocation; GPS-precision location additionally reveals home address, movement patterns, and the location at which a lottery ticket is purchased, none of which is necessary for the ticket-purchase function itself. No individually disclosed purpose for fine-location collection, consistent with the data minimisation requirement of Art. 5(1)(c), was identified in the available privacy documentation.

H4: Adjust (265 classes) + Adform (156 classes): dual, independent attribution SDKs on a state lottery

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)
 — two competing attribution processors doubling the external recipients of lottery-user behavioral data, neither individually named

com/adjust/sdk/	Adjust GmbH, Berlin / US infrastructure – 265 classes
com/adform/adformtrackingsdk/	Adform A/S, Copenhagen – 156 classes
com/adform/trackingsdk2/	

Impact: Two independent install- and behavioral-attribution SDKs run simultaneously: Adjust GmbH (Berlin, 265 classes) and Adform A/S (Copenhagen, 156 classes). Each independently receives lottery-user install and behavioral attribution data; running both doubles the number of external recipients of the same underlying data for no documented additional purpose. Neither Adjust nor Adform is individually named as a data processor in the available privacy documentation, and no Art. 44 transfer safeguard is identified for the portion of this data reaching Adjust's non-EU infrastructure.

H5: Salesforce Marketing Cloud processes lottery behavioral data for US-based CRM re-engagement campaigns

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)
 — a US marketing-CRM processor drives re-engagement campaigns from detailed lottery play-behavior data, in tension with the operator's own responsible-gambling duties

com/salesforce/marketingcloud/	Salesforce.com Inc., San Francisco, US
Behavioral signals processed: games played, purchase frequency, jackpot engagement patterns	
Art. 44 transfer safeguard: not identified	

Impact: Salesforce Marketing Cloud processes lottery-player behavioral data, which games are played, purchase frequency, and jackpot engagement patterns, on US infrastructure, to drive targeted re-engagement campaigns. For a state lottery operator with responsible-gambling obligations, CRM-driven re-engagement built on detailed play-behavior profiling is in direct tension with problem-gambling prevention duties, independent of the GDPR transparency gap. Salesforce Marketing Cloud is not individually disclosed as a data processor in the available privacy documentation.

Impact Analysis

Österreichische Lotterien's seven findings fall into two distinct categories. C1 and C2 are the two CRITICAL findings: C1 is a decision, not an oversight, the app deliberately instructs its entire user base to disable Android's sideload protection because the full version cannot be offered via Play Store under Google's policies, a trade-off made by a state operator that shifts security risk onto users, including the elderly and technically inexperienced demographics disproportionately represented among lottery players. C2 is a straightforward hardcoded-credential finding, but on a platform with active real-money gambling accounts.

The five HIGH findings share a common shape: Facebook (H1), the full Privacy Sandbox ad stack (H2), fine location (H3), dual attribution SDKs (H4), and Salesforce Marketing Cloud (H5) each represent an identifiable third-party data flow that is technically present and functioning but not individually disclosed with a lawful basis in the available privacy documentation. H2 and H5 in particular raise a question beyond GDPR: whether behavioral advertising profiling and CRM-driven re-engagement campaigns are compatible with a state lottery operator's own responsible-gambling obligations.

The Complete Chain: Disclosure Across Two Threads, 119 Days, Zero Substantive Replies

Step 1 — Disclosure sent: RFI-IRFOS sends the original findings to datenschutz@cal.at on 20 June 2026 under REF LOTTO-2026, CC help@lotterien.at, BCC the Austrian DSB and CERT.at.

Step 2 — First follow-up, same thread: On 27 June 2026, RFI-IRFOS follows up on the same thread, adding presse@lotterien.at to CC and restating the full finding set and embargo date. No substantive reply follows; only a generic autoresponse arrives from help@lotterien.at.

Step 3 — Parallel escalation track opened: With no substantive engagement from either address, RFI-IRFOS opens a second, parallel thread on 28 June 2026 addressed directly to help@lotterien.at and datenschutz@lotterien.at, Lotterien's own customer-facing and data-protection contact points, restating the complete disclosure and embargo date.

Step 4 — Repeated follow-ups, same silence: Further follow-ups in the second thread are sent on 5 August, 15 August, and 31 August 2026, each restating the unresolved finding set. Each of these generates its own disconnected, unthreaded autoresponse from help@lotterien.at, never a reply addressing any specific finding.

Step 5 — Embargo reached, then passed: The stated embargo of 19 September 2026 passes with the correspondence record unchanged across both threads: six messages sent, three generic autoresponses received, zero substantive replies.

Step 6 — Publication: This report publishes 28 days after the embargo date, on the terms stated from the first message.

Across two parallel threads and 119 days, the only responses Österreichische Lotterien's systems produced were three disconnected copies of the same autoresponse template. No named human at the state lottery operator ever addressed a single one of the seven findings.

Data Protection — Article by Article

Art. 32(1)(a)(b) GDPR — Security of processing: C1's sideload instruction and C2's hardcoded Firebase key both fall short of the technical measures Art. 32 requires, particularly for a platform with active real-money gambling accounts.

Art. 25(1) GDPR — Data protection by design: C1's choice to instruct users to disable a core Android security protection, in order to deliver the app's full functionality, is the inverse of privacy and security by design.

Art. 13 GDPR — Information to be provided, transparency: H1's Facebook/Meta data flow, H2's Privacy Sandbox pipelines, H3's fine-location collection, H4's dual attribution SDKs, and H5's Salesforce Marketing Cloud recipient are all undisclosed processing details Art. 13 requires to be communicated individually.

Art. 5(1)(c) GDPR — Data minimisation: H3's GPS-precision location collection exceeds what the stated jurisdictional-check purpose requires.

Art. 44 GDPR — General principle for transfers: H1, H4, and H5 each involve a third-country (US) data flow with no documented Art. 46 safeguard identified in the available privacy documentation.

Regulatory & Legal Landscape

Österreichische Lotterien GmbH is an Austrian state entity, placing it under the direct jurisdiction of the Österreichische Datenschutzbehörde (DSB), BCC'd on the original disclosure and every substantive follow-up. As a state-owned entity processing the gambling data of the Austrian population, Österreichische Lotterien carries an elevated duty of care beyond an ordinary commercial operator.

Fine exposure under GDPR: Art. 83(4) applies to the Art. 32/25 security-of-processing and design issues in C1 and C2, up to EUR 10,000,000 or 2% of total worldwide annual turnover. Art. 83(5) applies to the Art. 13 transparency and Art. 44 transfer issues in H1, H2, H4, and H5, up to EUR 20,000,000 or 4% of total worldwide annual turnover. Beyond GDPR, C1's sideload instruction may engage the Bundesministerium für Finanzen under GSpG technical-security requirements for licensed lottery operators, and H2's full Privacy Sandbox stack plus H5's CRM re-engagement campaigns present a novel regulatory fact pattern worth the gambling regulator's independent attention: advertising-driven re-engagement built on detailed play-behavior profiling, run by the state lottery operator itself.

Indicators of Compromise

The following identifiers, SDK packages, and credentials were extracted from the production APK (v4.7.0, versionCode 50983) via static analysis only. No Österreichische Lotterien servers, accounts, or infrastructure were probed.

```
C1 -- sideload-instruction dialog string, production update flow

C2 -- google_api_key AIzaSyDBPA6Fqixjq6RGP54GegQ1aqWfGuVmXDA,
    project_id gluecksbote-c9560

H1 -- com/facebook/* (1,234 classes incl. gamingservices, flipper),
    Meta Platforms Inc.

H2 -- ACCESS_ADSERVICES_TOPICS/CUSTOM_AUDIENCE/ATTRIBUTION/AD_ID,
    AD_ID (legacy)

H3 -- ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION

H4 -- com/adjust/sdk/ (265 classes), com/adform/* (156 classes)

H5 -- com/salesforce/marketingcloud/, Salesforce.com Inc.
```

Disclosure Timeline & Outcome

2026-06-20 Initial disclosure sent under REF LOTTO-2026 to datenschutz@cal.at, CC help@lotterien.at. BCC: Austrian DSB, CERT.at.

2026-06-27 Follow-up sent on the same thread, CC presse@lotterien.at added, full finding set and embargo date restated. Generic autoresponse received from help@lotterien.at; no substantive reply.

2026-06-28 Parallel escalation thread opened directly to help@lotterien.at and datenschutz@lotterien.at, restating the complete disclosure. No substantive reply.

2026-07-23 Generic autoresponse received from help@lotterien.at (standalone, unthreaded). No substantive reply.

2026-08-05 Follow-up sent in the escalation thread, restating the unresolved finding set. No reply.

2026-08-15 Follow-up sent in the escalation thread. Generic autoresponse received from help@lotterien.at (standalone, unthreaded). No substantive reply.

2026-08-31 Final follow-up sent in the escalation thread, restating the approaching embargo date. No reply.

2026-09-19 Stated embargo date reached. The correspondence record shows six RFI-IRFOS messages across two threads, three generic autoresponses, and zero substantive 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: Remove the sideload requirement entirely; deliver full app functionality, including Glücksbörse, via the Google Play Store or a transparent, Play-Protect-compatible alternative distribution channel, and reset affected users' "install from unknown sources" setting where technically feasible.

C2 — Immediate: Rotate the hardcoded Firebase API key and confirm the gluecksbote-c9560 project's security rules require authentication for all read and write operations.

H1 — Near-term: Remove the Flipper network debugger from the production build; conduct a scope review of the Facebook SDK, including Gaming Services, and execute a documented processor agreement with Meta.

H2 — Near-term: Document an individual Art. 6(1) lawful basis for each Privacy Sandbox pipeline, or remove the permissions not in active use.

H3 — Near-term: Replace GPS-precision location with IP-based jurisdictional geolocation, or document a specific purpose and minimisation justification for fine location.

H4 — Near-term: Consolidate to a single attribution provider where feasible, and execute documented processor agreements with both Adjust and Adform if dual attribution is retained.

H5 — Near-term: Individually disclose Salesforce Marketing Cloud as a processor with an Art. 44 transfer safeguard, and have the responsible-gambling compliance function independently review whether CRM-driven re-engagement campaigns built on play-behavior profiling are consistent with Österreichische Lotterien's own player-protection obligations.

Across all findings: establish a monitored intake path for security and data-protection disclosures that produces a substantive human response. Over 119 days and six messages across two separate threads, every response received was the same disconnected autoresponse template; no named human at the state lottery operator ever addressed a single finding.

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

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

of the published application using publicly available tooling. No Österreichische Lotterien servers, accounts, or infrastructure were probed. 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 LOTTO-2026.