



Security & Privacy Disclosure, Final Report

Supercell Android Portfolio (6 titles): Brawl Stars (com.supercell.brawlstars), Clash of Clans (com.supercell.clashofclans), Clash Royale (com.supercell.clashroyale), Hay Day (com.supercell.hayday), Boom Beach (com.supercell.boombeach), Squad Busters (com.supercell.squad)

Tencent Holdings, Supercell's 73%-majority shareholder, ships its own voice and multimedia SDK invisibly inside all six Supercell titles with no Art. 44 safeguard, while a shared Supercell ID silently links behavioral, spending, and social-graph data across the entire portfolio, unresolved through 116 days and a 25-day-overdue embargo, with every one of nine messages answered only by an automated helpdesk, never a human

PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 22 SEPTEMBER 2026, FOUR FINDINGS REMAIN UNADDRESSED

Target	Supercell Oy, Helsinki, Finland (majority-owned by Tencent Holdings Ltd., PRC)
Packages	com.supercell.brawlstars, com.supercell.clashofclans, com.supercell.clashroyale, com.supercell.hayday, com.supercell.boombeach, com.supercell.squad
Platform Audited	Android, portfolio-wide static analysis of all six production APKs
Initial Disclosure (R1)	2026-06-23 (REF ticket #368801286)
Disclosure / Embargo Date	2026-09-22
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	4 (2 Critical, 1 High, 1 Medium)
Correspondence	9 messages sent by RFI-IRFOS across five Helpshift-fragmented threads, 7 automated helpdesk autoresponses received, 1 bounce (info@cert.at), 0 substantive replies from privacy@supercell.com, dpo@supercell.com, or legal@supercell.com, or any named human
Authorities CC'd / BCC'd	Finnish Data Protection Ombudsman (tietosuoja@om.fi, lead supervisory authority, Supercell Oy registered Helsinki) · Austrian Datenschutzbehörde (DSB)

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: Tencent GME SDK, the majority shareholder's own voice and multimedia engine, embedded invisibly across all six titles with no Art. 44 safeguard . . .	6
4.2	C2: Supercell ID: an undisclosed cross-game behavioral profile linking all six titles via a shared content-provider permission	7
4.3	H1: Hay Day and Boom Beach: a disproportionate advertising-mediation SDK stack in the two titles most accessible to children	8
4.4	M1: android:allowBackup=true combined with hardcoded Firebase credentials across all six titles	9
5	Impact Analysis	9
6	The Complete Chain: A Disclosure Routed Into a Support Queue, Across Five Threads and 116 Days	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

Supercell Oy is a Finnish mobile games studio, 73%-majority owned by Tencent Holdings Ltd. of the People's Republic of China, operating a six-title portfolio with more than 2 billion combined downloads: Brawl Stars, Clash of Clans, Clash Royale, Hay Day, Boom Beach, and Squad Busters. A portfolio-wide static analysis of all six production Android binaries found four findings, two CRITICAL, one HIGH, one MEDIUM, that apply either across the full catalog or to the two titles rated accessible to children.

The majority shareholder's own SDK is embedded in every title. Tencent GME (Game Multimedia Engine), present as between 177 and 353 smali classes per app, handles real-time voice chat audio, device identifiers, and session metadata, and routes them through Tencent's infrastructure (C1). China's National Security Law Art. 7 obligates any PRC-registered entity to cooperate with state intelligence requests on demand; there is no GDPR adequacy decision for China and no disclosed Standard Contractual Clause covering this transfer. Separately, every title declares the `com.supercell.id.SHARED_DATA_ACCESS` content-provider permission and queries every other Supercell package at runtime, linking a single Supercell ID across the full portfolio into one aggregated behavioral profile of play frequency, session timing, spending, and social graph, a processing purpose never disclosed as a separate purpose in Supercell's privacy policy (C2). Hay Day and Boom Beach, rated Everyone and Teen respectively, carry a substantially larger advertising-mediation SDK footprint than the other four titles (IronSource, Facebook SDK, Unity Ads, AppLovin, Vungle, each between roughly 900 and 3,600 smali classes), none of which is individually named as a recipient in either app's privacy policy (H1). All six titles ship `android:allowBackup=true` alongside hardcoded Firebase credentials, enabling local backup extraction of app data on any device with ADB or physical access (M1).

RFI-IRFOS disclosed these findings on 23 June 2026 to privacy@supercell.com, CCdpo@supercell.com and legal@supercell.com, BCC the Finnish Data Protection Ombudsman (lead supervisory authority for Supercell Oy, registered in Helsinki) and the Austrian DSB. Supercell's Helpshift-based support platform routed the disclosure into a customer-service ticketing queue, fragmenting the correspondence across five separate thread IDs over the following 69 days and repeatedly auto-closing it as a duplicate or unrelated support ticket. Across that period RFI-IRFOS sent nine messages in total; seven automated Helpshift responses were received, along with one bounce (info@cert.at); not one human reply ever arrived. The report itself twice stated a different embargo date nine minutes apart (22 September in the main disclosure, 19 September in a same-day reply); per RFI-IRFOS's own internal consistency rule, the later of two dates we ourselves have stated governs, so the binding embargo is 22 September 2026, now 25 days overdue.

ID	Severity	Title
C1	CRITICAL	Tencent GME SDK, the majority shareholder's own voice and multimedia engine, embedded invisibly across all six titles with no Art. 44 safeguard
C2	CRITICAL	Supercell ID: an undisclosed cross-game behavioral profile linking all six titles via a shared content-provider permission
H1	HIGH	Hay Day and Boom Beach: a disproportionate advertising-mediation SDK stack in the two titles most accessible to children

ID	Severity	Title
M1	MEDIUM	android:allowBackup=true combined with hardcoded Firebase credentials across all six titles

Subject & Operator Context

Supercell Oy is a Helsinki-based mobile games studio founded in 2010, best known for Clash of Clans and Clash Royale and now operating a six-title catalog with a combined 2 billion plus downloads. In 2016, Tencent Holdings Ltd. of Shenzhen, China, acquired an 84.3% stake in Supercell, later reduced to approximately 73%, a majority holding Tencent retains today. Hay Day carries no minimum age rating on Google Play; Boom Beach is rated Teen. This audit treats the six titles as a single portfolio because the findings below either apply uniformly across all six binaries (C1, C2, M1) or specifically involve the two titles most exposed to younger players (H1).

Engagement Summary

RFI-IRFOS sent the initial disclosure on 23 June 2026 to privacy@supercell.com, dpo@supercell.com and legal@supercell.com, BCC the Finnish Data Protection Ombudsman and the Austrian DSB, under Helpshift ticket #368801286. Supercell's support platform immediately auto-replied with a generic in-game-purchases troubleshooting template; RFI-IRFOS replied the same day, nine minutes later, to put the misrouting on record.

From this point the correspondence fragments structurally, the same pattern already documented against other targets whose customer-service backend runs on a ticketing system rather than a flat mailbox: every new message to privacy@supercell.com opens or revives a distinct Helpshift thread ID, and several of RFI-IRFOS's follow-ups (23 and 24 July 2026) were met with an automated 'Issue Closed' notice stating the ticket had been closed as previously resolved, within minutes of being sent, before any human could plausibly have reviewed it. RFI-IRFOS sent further follow-ups on 24 July, 5 August, 15 August, 21 August, and 31 August 2026, each restating the open findings and noting the days elapsed. Across five separate Helpshift thread IDs and 69 days of active correspondence, RFI-IRFOS sent nine messages; Supercell's helpdesk auto-responded seven times (acknowledgments and closure notices), one message to info@cert.at bounced, and not one reply, automated or human, ever came from privacy@supercell.com, dpo@supercell.com, or legal@supercell.com directly addressing a single finding on its merits. The last message in the record, sent 31 August 2026, remains unanswered.

Findings

C1: Tencent GME SDK, the majority shareholder's own voice and multimedia engine, embedded invisibly across all six titles with no Art. 44 safeguard

CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 8.3) — real-time voice, device identifiers, and session metadata routed to a PRC entity bound by a state-cooperation law, across 2 billion plus downloads

```
Squad Busters (com.supercell.squad) -- GME: 353 smali classes
Hay Day (com.supercell.hayday) -- GME: 292 smali classes
Clash Royale (com.supercell.clashroyale) -- GME: 289 smali classes
Clash of Clans (com.supercell.clashofclans) -- GME: 241 smali classes
Boom Beach (com.supercell.boombeach) -- GME: 205 smali classes
Brawl Stars (com.supercell.brawlstars) -- GME: 177 smali classes

namespace: com.gme.*, com.gme.trtc, com.gme.liteav
operator: Tencent Holdings Ltd., PRC (approx. 73% shareholder of Supercell Oy)
```

Impact: Tencent GME (Game Multimedia Engine) is present in every one of the six audited titles, with class counts ranging from 177 (Brawl Stars) to 353 (Squad Busters) smali classes. Tencent Holdings Ltd. holds approximately 73% of Supercell Oy, making this the majority shareholder's own SDK, embedded invisibly across a 2-billion-plus-download portfolio. GME handles real-time voice chat audio, device identifiers, and session metadata, and routes them through Tencent's infrastructure in the People's Republic of China. China's National Security Law Art. 7 obligates any PRC-registered entity to cooperate with state intelligence requests on demand. There is no GDPR adequacy decision for China and no Standard Contractual Clause for this transfer identified anywhere in Supercell's available disclosures. Supercell's privacy policy does not name Tencent as a data recipient or disclose China as a transfer destination.

C2: Supercell ID: an undisclosed cross-game behavioral profile linking all six titles via a shared content-provider permission

CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 8.1) — a single identity silently aggregates play frequency, spending, and social-graph data across the entire portfolio with no disclosed legal basis for the aggregation itself

```
<package android:name="com.supercell.clashofclans"/>
<package android:name="com.supercell.clashroyale"/>
<package android:name="com.supercell.hayday"/>
<package android:name="com.supercell.boombeach"/>
<package android:name="com.supercell.squad"/>
<package android:name="com.supercell.moco"/>
<package android:name="com.supercell.id.SHARED_DATA_ACCESS"/>
```

Permission type: shared content provider, declared identically across all 6 titles
Disclosed as separate processing purpose: no

Impact: Every one of the six Supercell binaries declares the com.supercell.id.SHARED_DATA_ACCESS permission as a shared content provider and explicitly queries every other Supercell package at runtime (confirmed in the Brawl Stars manifest's <queries> block, which names com.supercell.clashofclans, com.supercell.clashroyale, com.supercell.hayday, com.supercell.boombeach, com.supercell.squad, and com.supercell.moco). A single Supercell ID links a player's behavioral data across the entire portfolio, which games they play, at what times, session duration, in-game purchasing behavior, and social graph, producing an aggregate profile considerably more detailed than any single title's own data. A Clash of Clans player has no way of knowing their behavioral data is linked to their Brawl Stars and Hay Day activity. Supercell's privacy policy describes data collection per game but does not disclose cross-game behavioral aggregation via Supercell ID as a separate processing purpose, as Art. 13(1)(c) requires.

H1: Hay Day and Boom Beach: a disproportionate advertising-mediation SDK stack in the two titles most accessible to children

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 ad-tech recipients collecting device identifiers and behavioral signals in a Everyone-rated and a Teen-rated title

Hay Day (com.supercell.hayday, rated Everyone):

IronSource (Unity Ads): 3,494 classes
 Facebook SDK: 3,594 classes
 Unity Ads: 2,651 classes
 AppLovin: 1,957 classes
 Vungle (Liftoff): 906 classes

Boom Beach (com.supercell.boombeach, rated Teen):

IronSource (Unity Ads): 3,324 classes
 Facebook SDK: 3,591 classes
 Unity Ads: 2,592 classes
 AppLovin: 1,570 classes
 Vungle (Liftoff): 863 classes

Named as data recipients in either app's privacy policy: no

Impact: Hay Day and Boom Beach carry a substantially larger third-party advertising SDK footprint than the other four Supercell titles: IronSource/Unity Ads, Facebook SDK, Unity Ads, AppLovin, and Vungle (Liftoff), each present as roughly 900 to 3,600 small classes per app. These are advertising-mediation platforms that collect device identifiers, behavioral signals, and contextual data to serve targeted advertising. Hay Day is rated Everyone on Google Play, with no minimum age restriction; Boom Beach is rated Teen. Advertising SDK stacks of this scale in games accessible to children raise specific concerns under GDPR Art. 8 and the EDPB Guidelines on children's data. Neither app's privacy policy enumerates IronSource, AppLovin, or Vungle as named data recipients, as Art. 13(1)(e) requires.

M1: android:allowBackup=true combined with hardcoded Firebase credentials across all six titles

MEDIUM (CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 4.0) — local backup extraction of app data and credentials by anyone with ADB or physical access to an unlocked device

```
AndroidManifest.xml (all 6 titles)
    android:allowBackup="true"
```

```
Hardcoded Firebase credentials present in each binary's resources
(specific keys withheld from this report pending Supercell's own
rotation; full detail available to Supercell's security team on request)
```

Impact: All six Supercell titles ship with `android:allowBackup=true`, permitting a full application-data backup via adb backup or an unlocked device's own backup tooling, alongside hardcoded Firebase credentials found embedded in each binary. Together these allow anyone with brief physical or ADB access to an unlocked device to extract locally stored application data and configuration credentials without needing to root the device or defeat any additional protection. This is a routine, fixable hardening gap rather than an actively exploited data breach, which is why it is scored MEDIUM rather than higher, but it sits alongside two CRITICAL findings in the same portfolio and should not be left unaddressed simply because it is the least severe of the four.

Impact Analysis

The two CRITICAL findings in this report share a structural root cause distinct from most audits in this disclosure series: they are not accidents of careless engineering, they are consequences of Supercell's ownership and product architecture. C1 exists because the majority shareholder embedded its own SDK into the product it controls, without naming itself as a recipient. C2 exists because Supercell deliberately built a unified identity system across its catalog, a legitimate product decision, without disclosing the behavioral-aggregation purpose that decision creates. H1 and M1 are more conventional gaps, an SDK-disclosure shortfall concentrated in the two titles most exposed to children, and a basic hardening omission repeated identically across all six binaries.

What ties all four together procedurally is the same failure that affected every other message in this record: a disclosure sent to a company's dedicated privacy address was never once engaged with by a human. Supercell's Helpshift-based support platform treated a formal GDPR notification exactly like a lost-account ticket, down to auto-closing it as resolved within minutes, repeatedly, over 69 days.

The Complete Chain: A Disclosure Routed Into a Support Queue, Across Five Threads and 116 Days

Step 1 – Disclosure sent: RFI-IRFOS sends the full portfolio disclosure to privacy@supercell.com on 23 June 2026, CC dpo@supercell.com and legal@supercell.com, BCC the Finnish Data Protection Ombudsman and the Austrian DSB. Helpshift ticket #368801286 is auto-created and immediately auto-replies with a generic in-game-purchases troubleshooting template.

Step 2 – On the record, same day: Nine minutes later, RFI-IRFOS replies to the automated responder directly, stating plainly that this is a regulatory GDPR matter, not a support ticket, and restating the coordinated disclosure deadline for the written record.

Step 3 – A bounce surfaces a second gap: The BCC to info@cert.at bounces the same day, undeliverable, address unknown, meaning Austria's own national CERT never received this disclosure through the address RFI-IRFOS used.

Step 4 – Thirty-one days of silence, then auto-closure: On 23 and 24 July 2026, RFI-IRFOS follows up restating the open findings. Supercell's helpdesk responds with 'Issue Closed' notices, twice in quick succession on 23 July, closing the ticket as previously resolved before any human review could plausibly have occurred.

Step 5 – Repetition across a new thread: A further follow-up on 24 July asks directly which of the three findings Supercell considers 'unrelated,' triggering another automated Helpshift acknowledgment and no substantive answer.

Step 6 – Continued silence through August: RFI-IRFOS sends further follow-ups on 5 August, 15 August, 21 August, and 31 August 2026, each restating the days elapsed and the findings still open. No human reply arrives at any point.

Step 7 – Embargo reached, then passed: The disclosure itself named two different dates nine minutes apart, 22 September in the main findings email and 19 September in the same-day reply to the automated responder. Per RFI-IRFOS's own internal rule that the later of two dates we ourselves have stated governs, the binding embargo is 22 September 2026, and it passed with all four findings unaddressed.

Step 8 – Publication: This report publishes 25 days after the embargo date. Across 116 days and nine messages sent, the only responses Supercell's systems produced were seven automated helpdesk messages and one closure notice stating the matter was resolved. It was never reviewed, let alone resolved.

Data Protection – Article by Article

Art. 44 GDPR – General principle for transfers: C1's Tencent GME data flow to the People's Republic of China has no adequacy decision and no disclosed Standard Contractual Clause.

Art. 13(1)(e), Art. 13(1)(f) GDPR – Information on recipients and third-country transfers: C1's Tencent is not named as a recipient, and China is not disclosed as a transfer destination, anywhere in Supercell's privacy policy.

Art. 13(1)(c), Art. 5(1)(a) GDPR – Purpose specification, lawfulness, fairness, and transparency: C2's cross-game behavioral aggregation via Supercell ID is never disclosed as its own distinct processing purpose.

Art. 13(1)(e) GDPR – Information on recipients: H1's advertising-mediation partners (Iron-Source, AppLovin, Vungle) are not individually named in either Hay Day's or Boom Beach's privacy policy.

Art. 32(1)(b), Art. 25(1) GDPR – Security of processing and data protection by design: M1's allowBackup=true plus hardcoded credentials falls short of the technical measures and by-design minimisation Art. 32 and Art. 25 require.

Regulatory & Legal Landscape

Supercell Oy is registered in Helsinki, Finland, placing it under the lead supervisory authority of the Finnish Data Protection Ombudsman (Tietosuojavaltuutetun toimisto), BCC'd on the original disclosure. The Austrian DSB was also BCC'd, given RFI-IRFOS's Austrian registration and the cross-border nature of a game catalog distributed to players across the EU.

Fine exposure under GDPR: Art. 83(5) applies to the Art. 44 and Art. 13 transparency and third-country-transfer issues in C1 and H1, and to the Art. 5(1)(a) purpose-limitation issue in C2, up to EUR 20,000,000 or 4% of total worldwide annual turnover. Art. 83(4) applies to the Art. 32 and Art. 25 security-and-design issue in M1, up to EUR 10,000,000 or 2% of total worldwide annual turnover. For a studio majority-owned by a PRC entity whose own SDK is the subject of the most severe finding in this report, the question of who is accountable for C1, Supercell Oy as the EU-facing controller, or Tencent as the SDK's operator and majority shareholder, is itself a fact a regulator will need to resolve, and one Supercell never engaged with across 116 days of correspondence.

Indicators of Compromise

The following identifiers, SDK packages, and permissions were extracted from the six production APKs via static analysis only. No Supercell servers, accounts, or infrastructure were probed.

```
C1 -- Tencent GME SDK (com.gme.*, com.gme.trtc, com.gme.liteav),  
    177-353 smali classes per title, all 6 titles  
  
C2 -- com.supercell.id.SHARED_DATA_ACCESS content-provider permission,  
    cross-app <queries> block naming all 6 Supercell packages  
  
H1 -- IronSource, Facebook SDK, Unity Ads, AppLovin, Vungle (Liftoff),  
    906-3,594 classes per SDK, Hay Day + Boom Beach only  
  
M1 -- android:allowBackup="true" + hardcoded Firebase credentials,  
    all 6 titles
```

Disclosure Timeline & Outcome

2026-06-23 Initial disclosure sent to privacy@supercell.com, CC dpo@supercell.com and legal@supercell.com, BCC Finnish DPO and Austrian DSB. Helpshift ticket #368801286 auto-created, auto-replies with an in-game-purchases template. RFI-IRFOS replies the same day to put the misrouting on record. BCC to info@cert.at bounces, undeliverable.

2026-07-23 Follow-up sent. Helpshift auto-closes the ticket as previously resolved, twice in quick succession, within minutes.

2026-07-24 Further follow-up asking which finding Supercell considers unrelated. Automated acknowledgment received, no substantive reply.

2026-08-05 Follow-up noting 43 days since the original disclosure. No reply.

2026-08-15 Follow-up noting 53 days since the original disclosure. No reply.

2026-08-21 Follow-up sent to privacy@supercell.com, CC dpo@supercell.com, legal@supercell.com, and the Austrian DSB. Automated acknowledgment received.

2026-08-31 Final follow-up sent, noting the fifth automated closure and 69 days since the original disclosure. No reply of any kind follows.

2026-09-22 Embargo date reached (the later of two dates stated in the original disclosure itself). The correspondence record shows nine RFI-IRFOS messages, seven automated Helpshift responses, and one bounce, zero substantive replies.

2026-10-17 This report published, 25 days after the embargo date. All four findings confirmed unaddressed on the basis of the correspondence record.

Residual Risk & Recommendations

C1 – Immediate: name Tencent Holdings Ltd. as a data recipient and China as a transfer destination in the privacy policy, and document a Standard Contractual Clause or equivalent Art. 44 safeguard for the GME voice and multimedia data flow, or remove the SDK from titles where real-time voice chat is not essential to gameplay.

C2 – Immediate: disclose cross-game behavioral aggregation via Supercell ID as its own distinct processing purpose under Art. 13(1)(c), with a documented legal basis, and offer players a way to opt out of cross-title linkage without losing access to any single game.

H1 – Near-term: name IronSource, AppLovin, and Vungle individually as data recipients in Hay Day's and Boom Beach's privacy policies, and review whether the scale of behavioral ad-tech in a Teen-rated and an unrated-for-age title is proportionate under GDPR Art. 8 and EDPB children's-data guidance.

M1 – Near-term: disable android:allowBackup or scope it to exclude sensitive data, and rotate the hardcoded Firebase credentials found in all six binaries.

Across all findings: establish a monitored intake path for security and data-protection disclosures that does not run through the same Helpshift queue used for lost-account and purchase-support tickets. Over 116 days and nine messages, every response Supercell's systems produced was an automated acknowledgment or a premature closure notice; the dedicated privacy mailbox itself never responded once, a process gap worth correcting independently of the four technical findings in this report.

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

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

of the six published applications using publicly available tooling. No Supercell 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 SUPERCELL-2026.