Security & Privacy Disclosure, Final Report

ClassDojo (com.classdojo.android)

A classroom app for schoolchildren that starts its analytics stack before any consent screen and records children's voice for an AI tutor, and an answer that points to a bug bounty queue.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026.

Target	ClassDojo, Inc., ClassDojo (Android app)
Version Audited	8.82.0 / versionCode 260088200 (analysed 2026-08-23)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	9: 2 High, 5 Medium, 2 Low (R1 labels reassessed, see status table)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`1dc0700fe0615455c00b3047e53fe3b23be8b98ad6eec82c0d8dd2c2f7fdfd62`

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

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

Contents

1 Executive Summary 3

2 Finding Status at a Glance 5

3 Subject & Operator Analysis 6

4 Architecture & Data Flow 6

5 Engagement Summary 7

6 Findings 7

6.1 C1: A Firebase and Google API key for the project dojopushnotifications is hard-coded in every distributed copy of the app . . . 7

6.2 C2: Firebase, Crashlytics and ML Kit start through manifest providers before any screen can render, with data collection forced on and no consent platform in the package . . . 8

6.3 H1: The operator's own text names the US COPPA school official exemption for school-based collection, and the roster flow shows no parent-facing consent strings . . . 9

6.4 H2: The paid Sparks AI reading tutor records children's voice responses and computes a named data category, Child AI Inferences . . . 10

6.5 H3: A Class Story post can tag several children and is shared with all parents and teachers in the class . . . 11

6.6 H4: The Data Safety card declares approximate location as collected and shared with third parties, while the manifest requests no location permission . 12

6.7 M1: The Sentry Session Replay module is bundled, and its sample rate and masking at runtime are not determinable from the package . . . 13

6.8 M2: Remote configuration with role-segmented feature flags, including grade-level targeting for the Sparks tutor . . . 13

6.9 M3: No certificate pinning is configured . . . 14

7 Impact Analysis 14

8 The Complete Chain 15

9 Child Protection 15

10 Data Protection: Article by Article 16

11 Platform Accountability & DSA 16

12 Regulatory & Legal Landscape 17

13 Indicators of Compromise & Reproducible Evidence 18

14 Disclosure Timeline & Outcome 19

15 What Was Done Well 19

16 Residual Risk & Recommendations 20

Executive Summary

ClassDojo is a classroom communication platform that connects teachers, parents and students. It is operated by ClassDojo, Inc. in San Francisco, has more than 50 million installs on Google Play, and is built on React Native. The users are schoolchildren in kindergarten to grade 8 and their families. On 23 August 2026 RFI-IRFOS sent a notice with REF CLASSDOJO-2026-R1 to privacy@classdojo.com, safety@classdojo.com and security@classdojo.com with the Austrian Datenschutzbehörde and the European Data Protection Supervisor in copy.

A root level code analysis of version 8.82.0 shows that the Firebase, Crashlytics and ML Kit providers start before any screen can render with data collection forced on, and that the package contains no consent platform (C2). A Firebase key is hardcoded (C1). The paid Sparks reading tutor records children's voice responses and computes a category that the operator itself calls Child AI Inferences (H2). The operator's own text rests school-based consent on the US school official exemption and the roster flow shows no parent-facing consent strings (H1). A Class Story post can tag several children and goes to every family in the class (H3). The Data Safety card declares approximate location while the manifest requests no location permission (H4). Three notes on session replay, remote configuration and certificate pinning complete the list (M1, M2, M3).

A reassessment by CVSS v4.0 band puts two findings at High, five at Medium and two at Low. The Critical label of C1 moves to Medium and that of C2 to High. H1, H3 and H4 move from High to Medium and H2 stays High. Each change is stated in the status table with its reason. Several things are done well, among them no advertising or attribution SDK, a deliberate disabling of the Sentry provider, and a 13 year threshold for a child's own login.

The operator answered the notice only with automated messages from the security mailbox and from the plus support desk, which point to a bug bounty programme on a third party platform. RFI-IRFOS replied on 25 August 2026, restated the three questions and received the same automated text. No substantive answer exists on 14 November 2026. This report is published on the embargo date of 21 November 2026.

Scope: Root level code analysis of the Google Play release 8.82.0 (versionCode 260088200) of ClassDojo, obtained from the APKPure mirror as an XAPK bundle and checked against the package name, developer and version on the live Google Play listing. The base APK of 108.3 MB was analysed, and the complete bundle with all splits is 157.6 MB. Work done: manifest and resource decode with apktool without source decode, string extraction across 7 classes dex files of about 60.6 MB, and string extraction from the 38.5 MB JavaScript bundle assets/index.android.bundle, which holds the application logic. The Google Play listing with the Data Safety card was read on 23 August 2026. No full bytecode disassembly was done, so code level statements rest on strings and are marked accordingly. The app was not installed, no account was created, no operator server was called and no traffic was captured. Findings that depend on runtime behaviour are marked as such.

ID	Severity	Title
C1	MEDIUM	A Firebase and Google API key for the project dojopushnotifications is hardcoded in every distributed copy of the app
C2	HIGH	Firebase, Crashlytics and ML Kit start through manifest providers before any screen can render, with data collection forced on and no consent platform in the package
H1	MEDIUM	The operator's own text names the US COPPA school official exemption for school-based collection, and the roster flow shows no parent-facing consent strings
H2	HIGH	The paid Sparks AI reading tutor records children's voice responses and computes a named data category, Child AI Inferences
H3	MEDIUM	A Class Story post can tag several children and is shared with all parents and teachers in the class
H4	MEDIUM	The Data Safety card declares approximate location as collected and shared with third parties, while the manifest requests no location permission
M1	MEDIUM	The Sentry Session Replay module is bundled, and its sample rate and masking at runtime are not determinable from the package
M2	LOW	Remote configuration with role-segmented feature flags, including grade-level targeting for the Sparks tutor
M3	LOW	No certificate pinning is configured

ID	Disclosed	This report	State on 14 November 2026

Finding Status at a Glance

ID	Disclosed	This report	State on 14 November 2026
C1	CRITICAL	MEDIUM	Autoreply, then a Bugcrowd redirect. Key restrictions not tested.
C2	CRITICAL	HIGH	Autoreply, then a Bugcrowd redirect. Data sent at start not observed.
H1	HIGH	MEDIUM	Autoreply, then a Bugcrowd redirect. Question 1 unanswered. Absence of strings only.
H2	HIGH	HIGH	Autoreply, then a Bugcrowd redirect. Question 2 unanswered. Consent timing UNVERIFIED.
H3	HIGH	MEDIUM	Autoreply, then a Bugcrowd redirect. Class-wide sharing is the declared function.
H4	HIGH	MEDIUM	Autoreply, then a Bugcrowd redirect. Question 3 unanswered. Mechanism UNVERIFIED.
M1	Not in notice	MEDIUM	Not in notice. Capability only.
M2	Not in notice	LOW	Not in notice. Capability only.
M3	Not in notice	LOW	Not in notice. Contextual note.

The notice of 23 August 2026 labelled C1 and C2 as Critical and H1 to H4 as High, and did not include M1, M2 and M3. This report uses the CVSS v4.0 band of each finding. C2 and H2 stay High through a blast-radius escalation that the finding states. A downgrade is made only where the evidence in the package or in the operator’s documents does not carry the earlier label.

Subject & Operator Analysis

The operator is ClassDojo, Inc., 735 Tehama Street, San Francisco, CA 94103, USA, an address that appears twice in the strings of the app bundle. The contacts are privacy@classdojo.com, support@classdojo.com, safety@classdojo.com and security@classdojo.com. The Play listing shows 50M+ downloads, 4.5 stars from 1.31 million reviews, the category Education, the content rating PEGI 3 with Users Interact, and in-app purchases. The data safety card says the operator is committed to follow the Play Families Policy.

The product is monetised through a subscription called ClassDojo Plus and a separately paid AI reading tutor called Dojo Sparks. The strings link a separate child privacy page and a Student Data Privacy Addendum aimed at US state student data privacy statutes.

No Article 27 representative in the Union was found in the strings of the package or in the privacy links bundled in the app. A search for EU representative, Art. 27, data protection officer and DPO found no hits. This statement covers the package only. The live privacy policy was not re-read for this report, so the absence of a representative is recorded as not found and not as established. No Union establishment of the operator was identified, so the one-stop-shop mechanism does not clearly apply and the Austrian Datenschutzbehörde can receive complaints directly.

Architecture & Data Flow

ClassDojo is a React Native app. The application logic sits in a minified JavaScript bundle of 38.5 MB, which the analysis read as strings, next to 7 classes dex files for the native layer. The minimum SDK is 26 and the target SDK is 36.

The Firebase stack is Messaging, Performance, RemoteConfig, Crashlytics with NDK, the Analytics connector, Sessions, Installations, Common, A/B Testing and Datatransport, registered through a direct boot aware discovery service and started by providers with init order 98 and 99 (C2). Datadog RUM and the Sentry Android SDK with its session replay module are bundled (M1). The advertising identifier collection of Firebase Analytics is switched off. No advertising or attribution SDK was found, and no Chinese or other sanctioned jurisdiction SDK appeared in about 330,000 extracted dex strings.

The network security configuration allows cleartext only for localhost and 127.0.0.1 and relies on the system trust store (M3). The microphone is used through RECORD_AUDIO for the Sparks feature (H2). The manifest holds no location permission (H4). The server side, the retention periods and the school agreements are not visible from the package.

Engagement Summary

The notice REF CLASSDOJO-2026-R1 was sent on 23 August 2026 at 14:33 UTC from rfi.irfos@gmail.com to privacy@classdojo.com, safety@classdojo.com and security@classdojo.com with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It carried six findings, a statement of what the product does well and three questions, and set the embargo date of 21 November 2026. Within seconds the security mailbox answered with an automated message that points researchers to a bug bounty programme and users to the help centre. On 25 August 2026 at 18:36 UTC the plus support desk, through its ticket system, wrote that vulnerability reports go through a bug bounty platform. RFI-IRFOS replied at 18:43 UTC the same day to the support desk with the three addresses in copy, restated the three questions and stated that the embargo date is unchanged. The security mailbox answered again with the same automated text. No further message exists and no delivery failure was returned.

Findings

C1: A Firebase and Google API key for the project dojopushnotifications is hardcoded in every distributed copy of the app

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N, 6.3 (CVSS-B), disclosed as CRITICAL on 23 August 2026

The file res/values/strings.xml holds the key as google_api_key and again as google_crash_reporting_api_key, with the Realtime Database URL and the project identifiers. Google documents such keys as identifiers and not as secrets. The exposure is availability, because anyone can extract the key and exhaust the API quota of the project, which backs the push channel that teachers and parents use. The security rules of the database were not tested, no call with the key was made, and the key restrictions are not visible from the package.

```
google_api_key                AIzaSyDex7HDNRyKuua1Rc13o4HFwUEZD-gyBbU
google_crash_reporting_api_key AIzaSyDex7HDNRyKuua1Rc13o4HFwUEZD-gyBbU
firebase_database_url         https://dojopushnotifications.firebaseio.com
google_app_id                 1:326575409030:android:841b985015ac3b73
project_id                    dojopushnotifications
default_web_client_id         326575409030-dh49kpvg69pqu07pldq2aj6aqlagm1rv.apps.
    googleusercontent.com
```

Impact: Anyone can read the key from the package in under a minute. Exhausting the quota of the project could slow or stop push notifications for all installs that share it, including time-sensitive messages between teachers and parents. Whether the project holds personal data of children is not shown.

Fix: Restrict the key by package name and signing certificate, review the database rules of the project, and move any privileged call to a server side component.

C2: Firebase, Crashlytics and ML Kit start through manifest providers before any screen can render, with data collection forced on and no consent platform in the package

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 (CVSS-B), disclosed as CRITICAL on 23 August 2026, rated HIGH by blast-radius escalation

Android starts content providers before any activity exists, in descending order of init order. The manifest declares the React Native Firebase app provider at 99, the Crashlytics provider at 98 and the ML Kit provider at 99, and forces app_data_collection_default_enabled, firebase_crashlytics_collection_enabled and firebase_messaging_auto_init_enabled to true. The component discovery service, which is direct boot aware, registers ten Firebase subsystems: Messaging, Performance, RemoteConfig, Crashlytics with NDK, the Analytics connector, Sessions, Installations, Common, A/B Testing and Datatransport. A search of the resources, of the dex strings and of the JavaScript bundle for OneTrust, Didomi, Usercentrics and IAB TCF identifiers found none, so the package holds no consent platform to gate these providers. The Sentry provider is switched off through io.sentry.auto-init false, so the pattern is not universal in this code base. What each provider transmits at start, and whether a consent or school agreement step precedes the first launch outside the app, was not observed. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the app has more than 50 million installs, its users are schoolchildren, and the start-up processing cannot be declined from inside the app.

```
<provider android:authorities="com.classdojo.android.
    reactnativefirebaseappinitprovider"
    android:exported="false" android:initOrder="99"
    android:name="io.invertase.firebase.app.ReactNativeFirebaseAppInitProvider"/>
<provider android:authorities="com.classdojo.android.
    reactnativefirebasecrashlyticsinitprovider"
    android:exported="false" android:initOrder="98"
    android:name="io.invertase.firebase.crashlytics.
    ReactNativeFirebaseCrashlyticsInitProvider"/>
<provider android:authorities="com.classdojo.android.mlkitinitprovider"
    android:exported="false" android:initOrder="99"
    android:name="com.google.mlkit.common.internal.MlKitInitProvider"/>

<meta-data android:name="firebase_crashlytics_collection_enabled" android:value="true
    "/>
<meta-data android:name="firebase_messaging_auto_init_enabled" android:value="true"/>
<meta-data android:name="app_data_collection_default_enabled" android:value="true"/>
```

Impact: The analytics, performance and crash reporting stack of the app starts at every process launch with collection enabled by default, and the package contains no mechanism that could ask anyone first. The app serves schoolchildren, and the age of digital consent in Austria is 14 under § 4 Abs. 4 DSG. A child or a parent cannot decline start-up collection from inside the app.

Fix: Disable collection by default, start the Firebase components only after the consent or school agreement decision is known, and document the legal basis for the start-up processing of children’s device data.

H1: The operator's own text names the US COPPA school official exemption for school-based collection, and the roster flow shows no parent-facing consent strings

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.3 (CVSS-B), disclosed as HIGH on 23 August 2026

The bundled privacy text in more than 15 languages states that parental consent for school-based services rests on the school official exemption of the US FTC COPPA rule, and says the operator extends US-style consent protections to all jurisdictions even if not legally required. The roster flow, where a teacher creates a student record with name, avatar, behaviour points and portfolio content, holds no consent, age gate or parental-consent strings in the bundle. The only age gate found controls the child's own invite and login at 13. This is an absence of strings in the app bundle. A consent step can sit in the school contract, in the web flow that invites a parent, or on the server, and a school can act as the controller. The app shows none of that.

```
"...Privacy Protection Rule (16 C.F.R. Part 312) (collectively "COPPA"), parental
consent is required for the collection, use or disclosure of personal information
from children [...] as allowed under COPPA - commonly referred to as the 'school
official' exemption..."

"ClassDojo extends the U.S.-based COPPA consent protections in all jurisdictions,
even if not legally required..."

"...your child's participation in the Sparks Feature and your child's participation
in the ClassDojo Outside School Services. We separately obtain COPPA consent for
school-based services as detailed in our FAQ..."
```

```
"Your teacher can send you a new invite once you turn 13. In the meantime, they
can always message your parents."

add_student_rostered_class, addStudentNameModalContent, add_students, add_student.
    submit
```

The school official exemption is a US instrument. Art. 8 of the GDPR asks for consent given or authorised by the holder of parental responsibility for information society services offered directly to a child. A school decision to adopt a tool is a different legal act. An operator could rely on Art. 6(1)(e) or 6(1)(f) through the school, but the text found describes the mechanism in COPPA terms only and names no Union legal basis.

Impact: The legal basis for the period between a teacher adding a child and any contact with a parent is not named in the operator's own text in Union terms. The affected group is schoolchildren on class rosters. Whether the school or the operator is the controller for that period, and what the school agreement says, are the open questions that the first question of the notice asks.

Fix: Name the Union legal basis for the roster stage and the controller and processor roles in the school agreement, and publish a consent or notice step for parents at the point the child record is created.

H2: The paid Sparks AI reading tutor records children's voice responses and computes a named data category, Child AI Inferences

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9 (CVSS-B), disclosed as HIGH on 23 August 2026, rated HIGH by blast-radius escalation

The operator's own text says that the child may record audio-only responses to Sparky's questions, that with consent the operator records them as Child Learning Assistant Audio and Text-Based Child Input, and that it may use Child AI Inferences to personalise the next interaction. The package has RECORD_AUDIO, the AudioRecord and MediaRecorder classes in dex, and JavaScript strings for native audio chunks, audio monitoring and speech assessment. The feature sits behind a subscription trial. The copy says that the feature depends on consent. When that consent is asked relative to the first audio chunk, and whether it is enforced equally for the school and the outside-school context, was not determined and is UNVERIFIED. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the feature records the voice of children, produces a named derived category over it, and runs in a product with more than 50 million installs.

```
"While interacting with the AI Learning Assistant throughout the Service, your
child may record audio-only responses to Sparky's questions or respond by
choosing pre-defined text-based answers. If you provide consent, ClassDojo
records those responses as Child Learning Assistant Audio and Text-Based Child
Input, collects information about your child's interactions with the AI
Learning Assistant, and may use Child AI Inferences to personalize the child's
next interaction with Sparky."

"Sparky listens as your child sounds out letters, offering real-time feedback
that builds both skills and confidence."

(SPARKS) Received native audio chunk, size: ...
(SPARKS) Using native module to stop audio monitoring, force: ...
useSpeechRecognitionMutation, useSparksSpeechAssessment, useSparksSubscription
SPARKS_TARGETING_THIRD_GRADE_OR_HIGHER_FEATURE_SWITCH, sparksTrialPurchaseDate
```

Impact: The product records the voice of children and builds a derived category from it that the operator itself names. A derived label over a child's speech can be more sensitive than the recording it comes from. The affected group is children of about the third grade and up, who use the tutor, and a household pays for the feature. The operator has not answered whether a data protection impact assessment exists, how long the audio and the inferences are kept, or when consent is asked.

Fix: Publish the data protection impact assessment, state the retention of audio and of the inference category, and ask for verified parental consent before the first microphone activation.

H3: A Class Story post can tag several children and is shared with all parents and teachers in the class

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.3 (CVSS-B), disclosed as HIGH on 23 August 2026

The strings of the story feed show a bottom sheet for tagged students and the text that the update will be shared with all parents and teachers in the class. A teacher who photographs a group activity captures every child in frame, and the post reaches every family on the class roster. A child whose guardian did not start or review the post is a bystander in the posting family's view of the data. The class is a closed group chosen by the school and the distribution is the declared function of the feature. Whether the guardians of every depicted child agreed elsewhere, for example in the school's photo consent, is not shown.

```
storyFeed:story_post.attachments.tagged_students_bottom_sheet.description
"Your update will be shared with all parents and teachers in the class."
"Your kid is tagged"
```

Impact: Images of children reach the families of classmates. The guardian of a depicted child receives the same post as everyone else and no separate notice for that image. The effect sits at the level of a school class and no public exposure is shown.

Fix: Let a guardian see and withdraw a tag of the child, and document the legal basis for sharing images of a child with all families in the class.

H4: The Data Safety card declares approximate location as collected and shared with third parties, while the manifest requests no location permission

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.3 (CVSS-B), disclosed as HIGH on 23 August 2026

The Data Safety section of the Play listing, read on 23 August 2026, lists Location as Approximate location under both data collected and data shared with third parties. The manifest declares no ACCESS_COARSE_LOCATION, ACCESS_FINE_LOCATION or ACCESS_BACKGROUND_LOCATION, confirmed by aapt badging and the decoded manifest. The app cannot obtain permission-gated coordinates, so the declared location can only come from another mechanism. The most plausible one is server side lookup from the network address, which was not confirmed from the package and is UNVERIFIED. The same card lists SMS or MMS messages and phone number as collected, and the manifest requests no SMS permission. That second point was not analysed further.

```
Play Data Safety: "Location - Approximate location" is listed under BOTH
"Data collected" and "Data shared [with third parties]"
```

```
DETECT_SCREEN_CAPTURE, USE_BIOMETRIC, WAKE_LOCK, CAMERA, RECORD_AUDIO,
MODIFY_AUDIO_SETTINGS, com.android.vending.BILLING, ACCESS_NETWORK_STATE,
INTERNET, RECEIVE_BOOT_COMPLETED, VIBRATE, WRITE_EXTERNAL_STORAGE (max SDK 32),
FOREGROUND_SERVICE, POST_NOTIFICATIONS, READ_EXTERNAL_STORAGE (max SDK 32),
c2dm.permission.RECEIVE, BIND_GET_INSTALL_REFERRER_SERVICE, ACCESS_WIFI_STATE,
DOWNLOAD_WITHOUT_NOTIFICATION, SCHEDULE_EXACT_ALARM,
BROADCAST_CLOSE_SYSTEM_DIALOGS (max SDK 30), ACCESS_NOTIFICATION_POLICY
```

Impact: A reader of the permission prompts sees no location access, while the operator discloses that location is collected and passed on. The mechanism and the recipients are not named. The point concerns transparency about derived location for the users of a children's product. No precise or background location is shown.

Fix: Name the mechanism and the recipients behind the declared location, and correct the Data Safety card if it is wrong.

M1: The Sentry Session Replay module is bundled, and its sample rate and masking at runtime are not determinable from the package

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), first stated in this report

The dex strings hold the complete session replay capture class tree of the Sentry Android SDK and its rrweb derived event classes, with the options maskAllText, maskAllImages, sessionReplaySampleRate and replaysOnErrorSampleRate. Capability is confirmed, runtime configuration is not. The app shows names, photos and portfolio content of children on screen throughout use. If replay were enabled at a non-zero sample rate without masking, recordings of that content would reach Sentry, a US vendor. The actual values are set at runtime, were not found as literals, and need dynamic instrumentation. Sentry's own automatic start is disabled in the manifest.

```
io/sentry/android/replay/capture/a  ... (full session-replay capture class tree)
Lio/sentry/rrweb/a; Lio/sentry/rrweb/b; ... RRWebBreadcrumbEvent.java, RRWebVideoEvent
    .java
maskAllImages, maskAllText, sessionReplaySampleRate, replaysOnErrorSampleRate
```

Impact: The module can record what a child sees in the app. Whether it is switched on is unknown, so the finding stays at capability level and asserts no transfer.

Fix: State the sample rates and masking defaults, and keep masking on by default for any replay in an app shown to children.

M2: Remote configuration with role-segmented feature flags, including grade-level targeting for the Sparks tutor

LOW, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B), first stated in this report

The bundle holds flag sets for teacher, student, parent and declined-school roles, local flags and defaults, and flags that target the Sparks feature by grade. Firebase RemoteConfig is registered by the component discovery service of C2. The operator can therefore change which features are active for a child account without an app update. This is an architectural fact. No exercised change that widens data collection was found, and none was sought, because no dynamic testing was done.

```
TEACHER_FEATURE_SWITCHES, STUDENT_FEATURE_SWITCHES, PARENT_FEATURE_SWITCHES
DECLINED_SCHOOL_FEATURE_SWITCHES, LOCAL_FEATURE_SWITCHES, FEATURE_SWITCHES_DEFAULTS
SPARKS_TARGETING_NO_GRADE_FEATURE_SWITCH_OVERRIDE
SPARKS_TARGETING_THIRD_GRADE_OR_HIGHER_FEATURE_SWITCH
```

Impact: A reader of the policy cannot tell that features, including the voice tutor, can change per role and grade without a release. No harm is shown.

Fix: Describe in the policy that features can change through remote configuration and that changes to the scope of processing are announced.

M3: No certificate pinning is configured

LOW, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B), first stated in this report

The network security configuration trusts the system store, allows cleartext only for localhost and 127.0.0.1, and confines the user certificate trust to debug builds. No pin set exists for any domain. This is common practice and not a defect by itself. It is noted because the same channels carry portfolio media of children, payment data and, for Sparks, recorded child audio. The finding is a contextual note.

```
<network-security-config>
    <domain-config cleartextTrafficPermitted="true">
        <domain includeSubdomains="false">localhost</domain>
        <domain includeSubdomains="false">127.0.0.1</domain>
    </domain-config>
    <base-config>
        <trust-anchors><certificates src="system" /></trust-anchors>
    </base-config>
    <debug-overrides>
        <trust-anchors><certificates src="user" /></trust-anchors>
    </debug-overrides>
</network-security-config>
```

Impact: An attacker who can place a certificate in the system store of a device could read traffic of the app. That needs control over the device or the network path.

Fix: Consider pinning for the endpoints that carry child media and audio.

Impact Analysis

The people affected are schoolchildren on class rosters, a population that is made up of children of roughly kindergarten to grade 8 age, and their families and teachers. Further people are classmates who appear in the photos and videos of a class story.

The weight of the case sits at three points. The analytics and crash stack starts at every launch with collection enabled and no consent platform can gate it (C2). The paid voice tutor records children and builds a named derived category from the speech (H2). The legal basis for the roster stage is described in US terms only (H1).

What the package shows is labelled capability, policy text and file content. No audio, image or identifier was observed leaving a device, and the report asserts no such flow.

The Complete Chain

Step 1, enrolment: a teacher adds a child to a class roster with name, avatar, points and portfolio content. The operator's text rests school-based consent on the US school official exemption and the roster flow shows no parent-facing consent strings (H1).

Step 2, start: the family or the teacher installs the app. The Firebase, Crashlytics and ML Kit providers start before any screen with collection forced on, and the package holds no consent platform (C2).

Step 3, use: the teacher posts class stories in which several children are tagged, and the posts go to all families in the class (H3). A household can buy the Sparks tutor, which records the child's voice responses and computes Child AI Inferences (H2).

Step 4, background: a session replay module, remote configuration flags and an unpinned TLS channel are present (M1, M2, M3). The Data Safety card declares approximate location, while the manifest requests none (H4).

Step 5, back end: a Firebase project with a key in every copy of the package serves push messages (C1).

Step 6, rights: the operator names no representative in the Union in the package, and a guardian who wants an answer meets an automated reply that points to a bug bounty queue.

Child Protection

The group at the centre of this case is schoolchildren in kindergarten to grade 8 whose teachers enrol them on class rosters. The child does not install the app, does not choose the product and does not read the policy. The Play rating PEGI 3 describes the content seen by the adult who installs it, and the rating scheme has no axis for the processing of the child. This report draws no conclusion from the number itself.

Protections exist and are credited. A child cannot receive an own invite or login before turning 13. The package contains no advertising or attribution SDK. The operator maintains a separate child privacy page and a student data privacy addendum. Sentry's own automatic start is disabled.

The open points are four. The legal basis for the roster stage is described in US terms only, and Austria sets the age of digital consent at 14 in § 4 Abs. 4 DSG, while the operator's policy defines no Union age threshold in the strings read. The start-up stack cannot be declined from inside the app. The voice tutor records children, and the timing of consent relative to the first audio capture is not determined. Class stories reach classmates' families. The operator's own text says it extends US style consent protections in all jurisdictions, which is credited, and the text does not say what a Union school or parent can rely on.

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C2, H1 and H4.

Article 5(1)(c), data minimisation: engaged by H4 and M2.

Article 5(2), accountability: engaged by C2.

Article 6: engaged by H1 for the roster stage and by H3 for bystander children. No Union legal basis for the roster stage is named in the text read.

Article 7(1): engaged by C2 as a question, because the operator may rely on a basis other than consent.

Article 8, children: engaged by H1 and H2. The text describes consent in COPPA terms and the Austrian age of digital consent is 14.

Article 9: engaged by H2 for children's voice and the derived category and by H3 for bystanders. No processing of special categories by the operator is asserted. The engagement is the sensitivity of the data.

Article 12 and Article 13: engaged by H4 for the declared location and by H3 for the guardians of bystander children.

Article 22: engaged by H2 for the personalisation loop over a minor.

Article 25: engaged by C1, C2 and M1.

Article 27: no representative in the Union was found in the package or in the bundled privacy links.

Article 28: engaged by M1 if replay data reaches Sentry.

Article 32(1)(a) and (b): engaged by M3 and C1.

Article 35: engaged by H1 and H2. No assessment was shown.

Platform Accountability & DSA

Google Play is an online platform under Regulation (EU) 2022/2065. Any person can submit a notice about an inaccurate Data Safety declaration under Art. 16 of that Regulation. RFI-IRFOS records the point here and treats the notice as a decision for the publication stage.

The Data Safety card of the Play listing declares approximate location as collected and shared (H4). It also lists SMS or MMS messages and phone number as collected, and the manifest requests no SMS permission. The Families Policy commitment on the card is not assessed in this report.

Regulatory & Legal Landscape

ClassDojo, Inc., a company in San Francisco, offers ClassDojo to users in the Union through Google Play, so Art. 3(2) of the GDPR applies. No main establishment in the Union is identified, so the one-stop-shop mechanism does not apply and the supervisory authority of each Member State where users are affected is competent under Art. 55. The Austrian Datenschutzbehörde (dsb@dsb.gv.at) and the European Data Protection Supervisor (edps@edps.europa.eu) received the notice in copy.

Infringements of Art. 5, 6, 7 and 9, of Art. 12 to 22 and of Art. 44 to 49 fall under the upper fine tier of Art. 83(5). Infringements of Art. 25, 27 and 32 fall under Art. 83(4). Data subjects can complain under Art. 77 and claim damages under Art. 82. Art. 5(3) of the ePrivacy Directive covers access to information on the user’s device. The notice of 23 August 2026 also cited Art. 33(4) as a question to the operator and no breach is asserted in this report.

The disclosure follows ISO/IEC 29147 and Art. 17 StGG. RFI-IRFOS acts under ZVR 1015608684 and GISA 39261441.

Indicators of Compromise & Reproducible Evidence

No indicators of compromise were found and none are claimed. The values below are the identifiers needed to reproduce each finding. All values are given in full.

```
Package            com.classdojo.android
Version            8.82.0 (versionCode 260088200), minSdk 26, targetSdk 36
Base APK size      108.3 MB (113,562,184 bytes)
Bundle size        157.6 MB (XAPK with all splits)
Base APK SHA-256   1dc0700fe0615455c00b3047e53fe3b23be8b98ad6eec82c0d8dd2c2f7fdfd62
XAPK SHA-256       ab2f516f2823985d35e10f5e87aabaaa99b4fd239b6c0372ab2316bdad88b147
Audit device       none, the app was not installed
Acquisition        APKPure mirror, checked against the Google Play listing, 2026-08-23
```

```
google_api_key                  AIzaSyDex7HDNRyKuua1Rc13o4HFwUEZD-gyBbU
google_crash_reporting_api_key  AIzaSyDex7HDNRyKuua1Rc13o4HFwUEZD-gyBbU
firebase_database_url           https://dojopushnotifications.firebaseio.com
google_app_id                   1:326575409030:android:841b985015ac3b73
project_id                      dojopushnotifications
default_web_client_id           326575409030-dh49kpvg69pqu07pldq2aj6aqlagm1rv.apps.
    googleusercontent.com
Contacts                        privacy@classdojo.com, support@classdojo.com,
    safety@classdojo.com, security@classdojo.com
Bug bounty address in the reply  https://bugcrowd.com/classdojo
Trust center in the reply        https://security.classdojo.com
```

```
C1  res/values/strings.xml
C2  AndroidManifest.xml (provider entries, meta-data), resource tree, dex and bundle
    strings (no consent platform)
H1  assets/index.android.bundle (privacy text, age gate and roster strings)
H2  assets/index.android.bundle (Sparks strings), AndroidManifest.xml (RECORD_AUDIO),
    dex (AudioRecord, MediaRecorder)
H3  assets/index.android.bundle (story feed strings)
H4  Play Data Safety card, AndroidManifest.xml (complete permission list)
M1  classes dex strings (io/sentry/android/replay, io/sentry/rrweb)
M2  assets/index.android.bundle (feature switch constants)
M3  res/xml/core_network_security_config.xml
```

Reproduction: obtain com.classdojo.android 8.82.0 (260088200), check the SHA-256 value above, decode manifest and resources with apktool without source decode, extract strings from the classes dex files and from assets/index.android.bundle, and read the Data Safety card of the Play listing. No device, account or network access is needed.

Disclosure Timeline & Outcome

2026-08-23 Notice REF CLASSDOJO-2026-R1 at 14:33 UTC to privacy@classdojo.com, safety@classdojo.com and security@classdojo.com, CC dsb@dsb.gv.at and edps@edps.europa.eu. Six findings, three questions, embargo date 21 November 2026.

2026-08-23 Automated reply from the security mailbox at 14:33 UTC that points to a bug bounty programme, a trust center and the help centre.

2026-08-25 Reply from the plus support desk at 18:36 UTC that vulnerability reports go through a bug bounty platform.

2026-08-25 Answer from RFI-IRFOS at 18:43 UTC to the support desk with the three addresses in copy. It restates the three questions and confirms the embargo date of 21 November 2026.

2026-08-25 Automated reply from the security mailbox at 18:44 UTC with the same text as before.

2026-11-14 No substantive reply, no answer to any of the three questions and no delivery failure.

2026-11-21 Embargo date, 90 days after delivery of the notice of 23 August 2026.

What Was Done Well

The network security configuration has no global cleartext permission. The only exception covers localhost and 127.0.0.1, and the user certificate trust is confined to debug builds. Firebase Analytics advertising identifier collection is switched off. Sentry’s own automatic start is disabled. No advertising or attribution SDK was found, and no Chinese or other sanctioned jurisdiction SDK appeared in about 330,000 dex strings. A child cannot receive an own invite or login before turning 13. A child privacy page and a student data privacy addendum are linked from the app. The target SDK is 36 and current. The operator extends US style consent protections in all jurisdictions, in its own words.

Residual Risk & Recommendations

Open at the date of publication: all nine findings. The operator has not answered the three questions of the notice. The largest open evidence gaps are the timing of consent for the voice tutor, the data sent at start, the runtime values of session replay, and the school agreements that decide who is the controller for the roster stage. A final APK diff against version 8.82.0 and a fresh reading of the privacy policy and of the Data Safety card before 21 November 2026 determine the state that the published report records.

Recommendations in order of effect. First, start the Firebase and ML Kit components only after the consent or school agreement decision (C2). Second, publish the impact assessment and the retention for the voice tutor and ask for verified parental consent before the first microphone activation (H2). Third, name the Union legal basis and the controller roles for the roster stage (H1). Fourth, let guardians see and withdraw tags of their child in class stories (H3). Fifth, explain the mechanism behind the declared location and correct the Data Safety card (H4). Sixth, restrict the Firebase key and state the replay settings (C1, M1). Seventh, describe remote configuration and consider pinning (M2, M3).

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 RFI-IRFOS research focus institute · ZVR 1015608684 ·

GISA 39261441 · Graz, Austria. Coordinated disclosure under ISO/IEC 29147, Art. 17 StGG (freedom of science) and Art. 89 GDPR. Root level code analysis of the published application only. CVSS values are CVSS v4.0 Base (CVSS-B) and model technical exposure, so transparency findings fit the scale only approximately. Labels above the computed band carry a blast-radius escalation statement in the finding. Final report, published 21 November 2026. REF CLASSDOJO-2026-R1.