Security & Privacy Disclosure, Final Report

Hailie, the patient app for the Hailie Smartinhaler asthma and COPD inhaler sensor, Android (com.smartinhalerlive)

A privacy policy that denies third-party analytics, an app that starts four of them first, and a children's product with a one-sentence safeguard.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO DATE 20 NOVEMBER 2026 REACHED. ONLY A HOLDING STATEMENT OF 16 SEPTEMBER 2026, NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026.

Target	Adherium (NZ) Limited, Auckland, New Zealand (parent Adherium Limited, ASX: ADR)
Versions Audited	10.6.6 / versionCode 4768, analysed 2026-08-21
Notice / Publication	2026-08-22 / 2026-11-20 (90 days)
Findings	6: 1 Critical, 4 High, 1 Medium
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`90f93709dad1cf3c31283a65548ed7856d05402a562714f321be73a5c60f623a`

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 4

3 Subject & Operator Analysis 5

4 Architecture & Data Flow 5

5 Engagement Summary 6

6 Findings 7

6.1 C1: The privacy policy says no third-party analytics are used, and the app starts four such processors before any consent screen . . . 7

6.2 C2: Cleartext traffic is permitted for every domain, and the package has no network security config and no pinning . . . 9

6.3 H1: A Firebase and Crashlytics key and the full Sentry DSN are hardcoded in every copy of the app . . . 10

6.4 H2: Mixpanel, Sentry, Auth0 and HappyFox are not named in the privacy policy, and support tickets can carry health context . . . 11

6.5 H3: The product is marketed for children, and the only minors safeguard is one sentence asking a parent to consent . . . 12

6.6 M1: The patient consent form is loaded in a WebView with the first name in the URL query string . . . 13

7 Impact Analysis 13

8 The Complete Chain 14

9 Children and Respiratory Health Data 14

10 Data Protection: Article by Article 15

11 Platform Disclosures: Google Play Data Safety 15

12 Regulatory & Legal Landscape 16

13 Indicators of Compromise & Reproducible Evidence 16

14 Disclosure Timeline & Outcome 17

15 What Adherium Got Right 17

16 Residual Risk & Recommendations 18

Executive Summary

Hailie is the patient app for the Hailie Smartinhaler, a Bluetooth sensor that clips onto an existing asthma or COPD inhaler and logs every dose to a cloud backend. Patients can join a programme managed by a healthcare professional. The app is published on Google Play under the package com.smartinhalerlive by Adherium (NZ) Limited of Auckland, the controller of record for users in the EU, EEA and UK. The Play listing says the solution reduces attacks in adults and children. On 22 August 2026 RFI-IRFOS disclosed findings from a root level code analysis of version 10.6.6 under REF HAILIE-2026-R1.

The sharpest finding is a contradiction between the privacy policy and the package. The policy states that Adherium does not use third-party service providers to monitor and analyse the use of the Services. The package starts Firebase Analytics, Firebase Crashlytics and Sentry through ContentProviders before any consent screen can appear, bundles Mixpanel, and configures Sentry for full trace sampling, full profiling and capture of the view hierarchy (C1). The package also permits cleartext traffic for every domain (C2), carries a Firebase key and the full Sentry DSN in clear text (H1), leaves four vendors unnamed in the policy (H2), relies on one sentence for the consent of minors (H3) and passes a first name in a URL (M1).

There is real care in the design. A purpose-specific consent screen guards the sharing of data with a healthcare professional. The dose database is encrypted with SQLCipher and Keystore and is excluded from backup. The Bluetooth permission model needs no location grant on current Android versions. No advertising SDK is present. A notice of 22 August 2026 listed the representative under Article 27 as a positive point. DataRep, the named representative, first said on 24 August that its appointment had ended, and confirmed on 14 September that it acts as the representative of Adherium (NZ) Limited. The question is closed and no finding rests on it.

The notice went to privacy@adherium.com with the representative, the Austrian DSB and the EDPS in copy. Adherium itself has sent one message since, a holding statement on 16 September 2026 that the matter was referred for internal review. Follow-ups on 12 September and 15 November 2026 restated the open questions. As of 21 November 2026 no finding and no question has been answered. This report is published after the embargo date of 20 November 2026 was reached.

Scope: Root level code analysis of the Google Play release 10.6.6 (versionCode 4768): manifest, resources, backup rules and the dex string pool of three classes*.dex files. The privacy policy at hailie.com/pages/privacy-policy and the Play listing were read from the public sites on 21 August 2026 and the policy was read again on 25 August 2026. No Adherium or Hailie server was called, no account was created, no sensor was paired, no traffic was captured and no runtime instrumentation was used. The companion app Hailie Care (com.adherium.hailierpm) was not analysed. Items the package cannot show are marked UNVERIFIED.

ID	Severity	Title
C1	CRITICAL	The privacy policy says no third-party analytics are used, and the app starts four such processors before any consent screen
C2	HIGH	Cleartext traffic is permitted for every domain, and the package has no network security config and no pinning
H1	HIGH	A Firebase and Crashlytics key and the full Sentry DSN are hardcoded in every copy of the app
H2	HIGH	Mixpanel, Sentry, Auth0 and HappyFox are not named in the privacy policy, and support tickets can carry health context
H3	HIGH	The product is marketed for children, and the only minors safeguard is one sentence asking a parent to consent
M1	MEDIUM	The patient consent form is loaded in a WebView with the first name in the URL query string

Finding Status at a Glance

ID	Disclosed	This report	Status on 21 November 2026
C1	CRITICAL	CRITICAL	Open. Questions 1 and 3 unanswered.
C2	CRITICAL	HIGH	Open. Question 2 unanswered.
H1	HIGH	HIGH	Open. No answer received.
H2	HIGH	HIGH	Open. No answer received.
H3	HIGH	HIGH	Open. No answer received.
M1	MEDIUM	MEDIUM	Open. No answer received.

Subject & Operator Analysis

The privacy policy names Adherium (NZ) Limited, PO Box 106612, Auckland 1143, New Zealand, as the controller for services provided directly to users in the EU, EEA and UK. The parent is Adherium Limited, ACN 605 352 510, PO Box 1149, Thornbury VIC 3071, Australia, listed on the Australian Securities Exchange (ADR). The policy names a data protection officer, whose contact is privacy@adherium.com and which matches the privacy_email string in the package. It names DataRep as the data protection representative for EU GDPR and UK GDPR, with the contact adherium@datarep.com. Support runs through adherium.happyfox.com.

The operator has no single EU main establishment. A representative under Article 27 does not create a lead supervisory authority, so for a matter that starts in Austria the Österreichische Datenschutzbehörde is competent. The Play listing shows 5,000 or more installs and was last updated on 10 November 2025. Adherium also publishes the newer app Hailie Care with about a fifth of the installs. It is outside this report.

Architecture & Data Flow

The app is a native Kotlin and Java application with Jetpack Compose and three dex files in a 28.2 MB package. It reads the Bluetooth LE sensor through RxAndroidBle and keeps the dose records in a SQLCipher database with keys wrapped by Android Keystore and Google Tink. The database and its preferences are excluded from backup in backup_rules.xml. Records go to regional clinical backends of the operator under hailie.com (us-go, hmp-us, hmp-uk, hmp-au, avillion and demo). No hmp-eu host was observed. Auth0 provides login with MFA, HappyFox provides support tickets, and a WebView loads the patient consent form from forms.adherium.com. Firebase Analytics, Crashlytics, Mixpanel and Sentry provide telemetry. The Bluetooth scan permission is declared with neverForLocation and the legacy location permissions are capped at SDK 30. The app has no advertising or ad mediation SDK.

Engagement Summary

The notice REF HAILIE-2026-R1 was sent on 22 August 2026 at 05:44 UTC to privacy@adherium.com, with adherium@datarep.com, dsb@dsb.gv.at and edps@edps.europa.eu in copy. It stated two critical findings in full, summarised three further findings, credited the design points set out below including the named representative, and asked three questions with a 14-day window.

On 24 August 2026 DataRep answered that it was no longer appointed as representative of the company. The same day RFI-IRFOS withdrew the credit for the representative and asked two further questions. On 25 August DataRep asked for the location of the declaration. RFI-IRFOS pointed to the Hailie-specific policy at hailie.com/pages/privacy-policy, which names DataRep. On 26 August DataRep answered that it would revert to the company.

On 12 September 2026 RFI-IRFOS sent a follow-up to privacy@adherium.com with five open questions and a deadline of 19 September 2026. On 14 September DataRep wrote that it was the data protection representative of Adherium (NZ) Limited and group companies and would pass the query on. The representative question was closed on that date. On 16 September 2026 an Adherium address answered with a holding statement, copied to a second Adherium address and to an external law firm. The statement says that the matter was referred for internal review and that the Adherium companies take privacy and security seriously. It addresses no finding and no question.

On 15 November 2026 at 12:59 UTC a final notice titled 5 days to publication went from s.kepp@rfi-irfos.com to privacy@adherium.com and a second Adherium address, with a third Adherium address, the external law firm and DataRep in copy, naming 20 November 2026 as the publication date. No further message from Adherium or its representative is on record as of 21 November 2026.

Findings

C1: The privacy policy says no third-party analytics are used, and the app starts four such processors before any consent screen

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 22 August 2026, open, rated CRITICAL by blast-radius escalation

The policy read on 21 August 2026 at hailie.com/pages/privacy-policy states under Reasons We Use Your Personal Data: "Adherium does not currently use third-party service providers to monitor and analyze the use of the Services." The package declares and wires in Firebase Analytics, Firebase Crashlytics, Mixpanel and Sentry, and opens Google's AdServices attribution channel to all callers (allowAllToAccess true). FirebaseInitProvider (directBootAware, initOrder 100), CrashlyticsInitProvider (initOrder 100) and SentryPerformanceProvider (initOrder 200) are ContentProviders, so they start with the process before any Activity and before any consent screen. Sentry is set to a trace sample rate of 1.0, a profiling sample rate of 1.0 and attach-view-hierarchy true, with an ingest endpoint in the US, for an app whose screens show dose history and account identifiers. Mixpanel has no ContentProvider, and its first call relative to the consent screen is UNVERIFIED. Its endpoints and MPConfig metadata show that it is bundled and configured, and the policy's blanket denial covers it regardless of timing. What the telemetry contains was not measured and no traffic was captured. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to CRITICAL because the app serves people with asthma and COPD including children, a statement in the controller's own legal document is disproved by its own binary, and Sentry captures the structure of screens that show doses. The CVSS vector scores only the technical exposure of low-sensitivity telemetry.

```
Adherium does not currently use third-party service providers to monitor and analyze
the use of the Services.
```

```
<provider android:authorities="com.smartinhalerlive.firebaseinitprovider"
          android:directBootAware="true" android:exported="false"
          android:initOrder="100" android:name="com.google.firebase.provider.
    FirebaseInitProvider"/>
<provider android:authorities="com.smartinhalerlive.crashlyticsinitprovider"
          android:exported="false" android:initOrder="100"
          android:name="com.crashlytics.android.CrashlyticsInitProvider"/>
<provider android:authorities="com.smartinhalerlive.SentryPerformanceProvider"
          android:exported="false" android:initOrder="200"
          android:name="io.sentry.android.core.SentryPerformanceProvider"/>
<provider android:authorities="com.smartinhalerlive.SentryInitProvider"
          android:exported="false" android:name="io.sentry.android.core.
    SentryInitProvider"/>
<meta-data android:name="io.sentry.traces.sample-rate" android:value="1.0"/>
<meta-data android:name="io.sentry.traces.profiling.sample-rate" android:value="1.0"/>
<meta-data android:name="io.sentry.attach-view-hierarchy" android:value="true"/>
<meta-data android:name="com.mixpanel.android.MPConfig.UseIpAddressForGeolocation"
    android:value="false"/>
<property android:name="android.adservices.AD_SERVICES_CONFIG" android:resource="@xml/
    ga_ad_services_config"/>

res/xml/ga_ad_services_config.xml:
<ad-services-config><attribution allowAllToAccess="true" /></ad-services-config>
```

```
https://app-measurement.com/a
https://app-measurement.com/s
https://app-measurement.com/s/d
https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/
https://e.crashlytics.com/spi/v2/events
https://api.mixpanel.com/track
https://api.mixpanel.com/engage
https://decide.mixpanel.com/decide
```

Impact: A parent who registers a child’s asthma inhaler, or an adult who tracks COPD doses, reads a policy that says nobody outside the company monitors the use of the app. Four outside companies receive usage signals from the first second the app runs, and one of them records the structure of the screens that show prescriptions and doses.

Fix: Correct the privacy policy to name every processor, start Firebase, Crashlytics, Sentry and Mixpanel only after a recorded consent decision, and reduce Sentry sampling and view hierarchy capture for screens that show health data.

C2: Cleartext traffic is permitted for every domain, and the package has no network security config and no pinning

MEDIUM, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 6.0 (CVSS-B), disclosed as CRITICAL on 22 August 2026, open, rated HIGH by blast-radius escalation

The application element sets android:usesCleartextTraffic to true. This is an explicit override, because a targetSdk 35 app that omitted the attribute would deny cleartext by default. res/xml/ holds no network_security_config.xml, so there is no domain list, no scoped exception and no pin for any host, among them the operator's own backends us-go.hailie.com, hmp-us.hailie.com, hmp-uk.hailie.com, hmp-au.hailie.com, avillion.hailie.com and demo.hailie.com. Every endpoint string that the analysis extracted begins with https. The package permits a fall back to unencrypted HTTP and does not show that one occurs. The notice of 22 August 2026 rated this finding CRITICAL. This report rates it HIGH, because a permission to use cleartext is not shown to be exercised. No traffic was captured. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.0 to HIGH because the data is medication adherence data, which is health data under Article 9, and the setting is a deliberate override with no compensating restriction. The CVSS vector scores the attacker position that is required on a local network.

```
<application android:allowBackup="false" ... android:usesCleartextTraffic="true">

res/xml/network_security_config.xml : absent

Backends seen in the string table: us-go.hailie.com, hmp-us.hailie.com, hmp-uk.hailie.
    com,
hmp-au.hailie.com, avillion.hailie.com, demo.hailie.com  (hmp-eu not observed)
```

Impact: The payload is the time of every inhaler dose. On a hostile network, such as a public hotspot, a downgrade to plain HTTP would expose when and how often a person with a respiratory condition takes medication.

Fix: Set usesCleartextTraffic to false, add a network security config that denies cleartext for all hosts and add pins for the operator's own backends.

H1: A Firebase and Crashlytics key and the full Sentry DSN are hardcoded in every 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 HIGH on 22 August 2026, open, rated HIGH by blast-radius escalation

The Firebase key for the project hailie-primary, with its storage bucket hailie-primary.appspot.com, the Crashlytics API key and the full Sentry DSN sit in clear text in the distributed package. Google documents Firebase keys as non-secret by design, so this is an availability finding and not a confidentiality finding. An extracted key can be used to exhaust the quota of the project. The Sentry DSN and the Crashlytics key are write tokens of the same class. Whether the Security Rules and the storage bucket are locked down is not shown by the package, and no call was made against either key, the project or the DSN. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.3 to HIGH because the project belongs to a patient-facing medication app, and the key cannot be rotated for installed copies. The CVSS vector scores only the availability exposure that the package demonstrates.

```
<string name="google_api_key">AIzaSyAXHcwWRU2S5MaZ_HIwIGbMh3mDHpYvgqM</string>
<string name="google_crash_reporting_api_key">AIzaSyAXHcwWRU2S5MaZ_HIwIGbMh3mDHpYvgqM
    </string>
<string name="google_app_id">1:966094863875:android:30e835b63d2a66a52e5836</string>
<string name="project_id">hailie-primary</string>
<string name="google_storage_bucket">hailie-primary.appspot.com</string>
<string name="gcm_defaultSenderId">966094863875</string>
<string name="default_web_client_id">966094863875-6fqqcstgg9r19j84sundf5anh17lcre9.
    apps.googleusercontent.com</string>

<meta-data android:name="com.crashlytics.ApiKey" android:value="7
    ecb5bd6d5f09465deec5b36e116f5689e27edba"/>
<meta-data android:name="io.sentry.dsn" android:value="https://02326
    c98886a30ab87e9543e18657310@o1060637.ingest.us.sentry.io/4507175218118656"/>
```

Together with the Sentry settings in C1, an actor holding the DSN can send events into the operator's own crash monitoring. The DSN does not read data from it.

Impact: The key cannot be rotated for installed copies without an app update. If the project is rate-limited or billed out, crash reporting and the services that run on the project stop. For a medication app, the open point is whether the storage bucket of the project is closed to outsiders.

Fix: Restrict the keys by package name and signing certificate, enforce App Check, rotate the DSN, and send the Security Rules and bucket settings as evidence.

H2: Mixpanel, Sentry, Auth0 and HappyFox are not named in the privacy policy, and support tickets can carry health context

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), disclosed as HIGH on 22 August 2026, open, rated HIGH by blast-radius escalation

The policy section on disclosing or sharing personal information names two processors: Shopify and an unnamed payment processor. It adds a general clause that certain third party data processors provide aspects of the Services. The package contains Auth0 for login with MFA flows (mfa-oob, mfa-otp, mfa-recovery-code), HappyFox for support ticketing at adherium.happyfox.com, Mixpanel for behavioural analytics and Sentry for crash and performance monitoring. None is named in the policy text obtained. A general clause does not meet the duty to name recipients or categories of recipients for four identifiable vendors with four different data scopes. HappyFox may receive free text from users who describe a health condition. This is a transparency finding with no technical attack path, so the CVSS vector carries no impact. RFI-IRFOS blast-radius escalation: raised from none to HIGH because the vendors receive login data, behavioural data and support text from patients, and the policy names none of them. The score is zero because no technical vector exists.

```
com.auth0.android.provider.RedirectActivity / AuthenticationActivity   (Auth0, login
    and MFA)
HAPPYFOX_API / HAPPYFOX_CATEGORY_ID / HAPPYFOX_PRIORITY_ID / HAPPYFOX_SUPPORT_EMAIL
https://adherium.happyfox.com                                          (HappyFox,
    support tickets)
com.mixpanel.android.MPConfig                                           (Mixpanel,
    analytics)
io.sentry.android.core                                                  (Sentry, crash
     and performance)
```

Impact: A patient who writes to support about a symptom or a child's asthma attack sends that text to a ticketing vendor that the policy does not name.

Fix: Name each processor, its role and the data it receives in the privacy policy, and state which of them receive support free text.

H3: The product is marketed for children, and the only minors safeguard is one sentence asking a parent to consent

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), disclosed as HIGH on 22 August 2026, open, rated HIGH by blast-radius escalation

The Play listing states that clinical evidence shows that the Hailie solution increases adherence and reduces attacks ”in adults and children”. Registration collects a date_of_birth field. The only minors safeguard in res/values/strings.xml (privacy_consent) is the sentence: ”For any user under the age of majority a parent or legal guardian must provide the consent below.” No blocking step, no document or behaviour based age assurance and no string for an age limit or a parental verification workflow was found, and nothing shows that the date of birth gates any feature. Article 8 asks the controller to make reasonable efforts to verify that the holder of parental responsibility gave or authorised consent. A self-declared instruction on the same screen that a child can use is not shown to meet that standard. No exploitation is claimed. This is a legal and design finding with no technical attack path, so the CVSS vector carries no impact. RFI-IRFOS blast-radius escalation: raised from none to HIGH because the audience includes children with a chronic respiratory condition and the data is their medication record. The score is zero because no technical vector exists.

```
Play listing: "...reduces attacks in adults and children."

res/values/strings.xml (privacy_consent):
  "For any user under the age of majority a parent or legal guardian must provide the
   consent below."
```

Impact: A child with asthma can reach the consent screen alone. Nothing in the app checks who taps the consent, although the data describes the child’s medication and the app starts four outside processors before that screen appears.

Fix: Add a verifiable parental consent step for users under the age of majority, gate registration on the date of birth and document the method used.

M1: The patient consent form is loaded in a WebView with the first name in the URL query string

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), disclosed as MEDIUM on 22 August 2026, open

The registration step for patient consent loads an externally hosted form at forms.adherium.com/patient-consent in an embedded WebView (PatientConsentWebView, RegisterConsentScreenKt$RegisterWebView) and passes the user's first name as a query parameter. URLs are commonly stored in web server logs, browser history and intermediary logs, and can reach third-party resources through the Referer header. A first name alone is low in sensitivity. The channel is weaker than a request body for a screen that exists to capture consent for health data sharing.

```
https://forms.adherium.com/patient-consent?firstname=...
```

Impact: A patient's first name, tied to a health consent form, can end up in server logs and history entries that nobody planned for.

Fix: Send the name in the body of an authenticated request or leave it out of the URL, and set a strict referrer policy on the form.

Impact Analysis

The people affected are patients with asthma and COPD who log inhaler doses, and the parents of children who do. The data describes when and how often a person takes medication, which shows the state of a chronic condition. In a household with a child, the parent registers the sensor and the child may use the app.

The most direct harm is a false picture. A policy that says no third party monitors use tells the family one thing, while four outside processors receive signals and one of them captures screen structure (C1, H2). A permission for cleartext traffic gives a local attacker a way to downgrade a connection that carries dose times (C2). A child is asked to take part in a consent step with one sentence of guidance (H3).

The Complete Chain

Step 1, install: a patient or parent installs the app from Google Play. The label says no data is shared with third parties and the policy says no third-party monitoring is used (C1).

Step 2, process start: Firebase, Crashlytics and Sentry start as ContentProviders before any screen. Mixpanel is bundled, and its start is UNVERIFIED (C1).

Step 3, registration: the user creates an account through Auth0 and enters a date of birth. A consent form loads in a WebView with the first name in the URL (M1). A sentence asks a parent to consent for a minor (H3).

Step 4, use: the sensor reports doses over Bluetooth, the app stores them in an encrypted local database and sends them to a regional backend. The configuration permits cleartext for every host (C2).

Step 5, support: a patient writes to support and the text reaches HappyFox, which the policy does not name (H2).

Step 6, programme: the user may join a healthcare professional programme through a code, after a purpose-specific consent screen that names the data shared.

Step 7, infrastructure: the project key and the Sentry DSN sit in every copy of the app (H1).

Children and Respiratory Health Data

The listing speaks to the care of children with asthma. Medication records of a child are health data of a person who cannot consent alone. Article 8 sets the age of digital consent per Member State and asks for reasonable efforts to verify parental authority where consent is the legal basis.

The package collects a date of birth and shows no use of it as a gate. The consent screen speaks to the user and asks a parent to give the consent below. The same screen is reachable by the child. This report claims no misuse and records the gap between the audience of the product and the control in the app.

The categories of household graph, notification relationships and non-events do not apply. The sensor is worn on one inhaler for one patient and the package has no household feature.

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1 and H2.

Article 5(1)(c), data minimisation: engaged by H3.

Article 5(1)(f) and Article 32(1)(a) and (b), integrity, confidentiality and security of processing: engaged by C2, H1 and M1.

Article 5(2), accountability: engaged by C1. The controller must be able to show that its stated processing map is correct.

Article 7(1), conditions for consent: engaged by C1, where processing that rests on consent starts before the consent screen.

Article 8, child's consent: engaged by H3.

Article 9, special categories: the dose records are health data and frame C1, C2 and H3.

Article 13(1)(e), recipients: engaged by C1 and H2.

Article 24 and Article 25, responsibility of the controller and data protection by design: engaged by H1 and H3.

Article 27, representative: not engaged. The representative named in the policy confirmed its role on 14 September 2026.

ePrivacy Directive Art. 5(3): engaged by C1, because storing or reading information on terminal equipment needs consent unless strictly necessary.

Platform Disclosures: Google Play Data Safety

The Data Safety label is a declaration made by the developer in Google Play Console. This report attributes it to the developer and makes no claim about the platform operator.

The label states in unqualified terms that no data is shared with third parties. The policy separately describes sharing with a healthcare professional under a programme code. The package shows a purpose-specific, opt-in consent screen for that sharing, and under the platform's own taxonomy a transfer made at the user's direction to a treating clinician plausibly falls outside third-party sharing. The statement is much harder to defend once Firebase Analytics, Crashlytics, Mixpanel and Sentry are counted, because those are independent companies that receive usage data for their own service operation. The label was read in August 2026 and the page was not archived. It should be fetched again before publication.

Regulatory & Legal Landscape

The framework applied is the GDPR with Article 9 for health data, Article 8 for children, Article 13 for information and Article 32 for security, together with Article 5(3) of the ePrivacy Directive for terminal equipment. The operator is established in New Zealand and offers its product to users in the Union, which brings Article 3(2) GDPR into play. DataRep, established in Ireland, acts as the representative under Article 27 and is named in the policy.

No single EU main establishment exists, so each concerned supervisory authority is competent. The Österreichische Datenschutzbehörde (dsb@dsb.gv.at) is the authority for a matter that starts in Austria. The European Data Protection Supervisor (edps@edps.europa.eu) is in copy under the standing practice of the programme. The disclosure follows ISO/IEC 29147 and Art. 17 StGG. No obligation under other digital regulation is asserted, because the classification of the operator and the product has not been established.

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 from the published package. All values are given in full.

```
Package            com.smartinhalerlive
Version            10.6.6 (versionCode 4768), analysed 2026-08-21
minSdk / target    23 / 35
APK size           29,531,900 bytes
APK SHA-256        90f93709dad1cf3c31283a65548ed7856d05402a562714f321be73a5c60f623a
Firebase project   hailie-primary
Firebase API key   AIzaSyAXHcwWRU2S5MaZ_HIwIGbMh3mDHpYvgqM (google_api_key and
    google_crash_reporting_api_key)
Google app ID      1:966094863875:android:30e835b63d2a66a52e5836
Storage bucket     hailie-primary.appspot.com
Sender ID          966094863875
Web client ID      966094863875-6fqqcstgg9r19j84sundf5anh17lcre9.apps.
    googleusercontent.com
Crashlytics key    7ecb5bd6d5f09465deec5b36e116f5689e27edba
Sentry DSN         https://02326c98886a30ab87e9543e18657310@o1060637.ingest.us.sentry.
    io/4507175218118656
Operator           Adherium (NZ) Limited, Auckland
```

```
C1  hailie.com/pages/privacy-policy (read 2026-08-21). AndroidManifest.xml: four
    providers, Sentry and Mixpanel meta-data. res/xml/ga_ad_services_config.xml
C2  AndroidManifest.xml: usesCleartextTraffic. res/xml/: no network_security_config.
    xml
H1  res/values/strings.xml, AndroidManifest.xml: keys and DSN
H2  Policy section on disclosing or sharing personal information. classes*.dex: Auth0,
     HappyFox, Mixpanel, Sentry
H3  Play listing text. res/values/strings.xml: privacy_consent
M1  classes*.dex: PatientConsentWebView, RegisterConsentScreenKt$RegisterWebView
```

Reproduction: obtain com.smartinhalerlive 10.6.6 from Google Play, check the SHA-256

above, decode the manifest and resources with apktool and read the named files. No device, account or network access is needed for the package findings.

Disclosure Timeline & Outcome

2026-08-22 Notice REF HAILIE-2026-R1 to privacy@adherium.com, CC adherium@datarep.com, DSB and EDPS. Two critical findings in full, three more summarised, three questions asked, reply requested within 14 days.

2026-08-24 DataRep replies that it is no longer appointed as representative. RFI-IRFOS withdraws the credit for the representative and asks two further questions.

2026-08-25 DataRep asks for the location of the declaration. RFI-IRFOS names the Hailie-specific policy at hailie.com/pages/privacy-policy as the source.

2026-08-26 DataRep replies that it will revert to the company.

2026-09-12 Follow-up to privacy@adherium.com with five open questions, deadline 19 September 2026, embargo named as 20 November 2026.

2026-09-14 DataRep writes that it is the data protection representative of Adherium (NZ) Limited and group companies and passes the query on. The representative question is closed.

2026-09-16 Holding statement from an Adherium address, copied to a second Adherium address and an external law firm. The matter is referred for internal review. No finding or question addressed.

2026-11-15 Final notice from s.kepp@rfi-irfos.com to privacy@adherium.com and a second Adherium address, copied to a third Adherium address, the external law firm and DataRep, naming 20 November 2026 as the publication date. No reply followed.

2026-11-20 Embargo date, 90 days after delivery of the notice of 22 August 2026. No message from Adherium after the holding statement of 16 September 2026 is on record as of 21 November 2026.

What Adherium Got Right

A purpose-specific, opt-in consent screen (group_code_user_consent) names what is shared with a healthcare professional and with whom, before any programme enrolment takes effect. No advertising or ad mediation SDK is present. The Bluetooth permission model is current and the app needs no location permission on Android 12 and later. The dose database is encrypted with SQLCipher and Android Keystore through Tink and is excluded from backup, so the most sensitive payload is the best protected data on the device. allowBackup is false. The app locks with BiometricPrompt and Keystore, supports MFA through Auth0 and checks password strength on registration. The policy names an EU and UK representative with working contact details, and DataRep confirmed its role on 14 September 2026. A data protection officer is named with a working address.

Residual Risk & Recommendations

Open at the date of publication: all six items, with no written position from the operator. Items that only the operator can close are the policy and consent gate in C1, the network security config in C2, the key restrictions and DSN in H1, the processor list in H2, the parental consent method in H3 and the URL handling in M1.

Recommendations: correct the policy to name every processor, start telemetry only after a recorded consent decision and reduce Sentry sampling on screens that show health data, deny cleartext and pin the operator’s hosts, restrict the Firebase key and rotate the DSN, name Auth0, HappyFox, Mixpanel and Sentry, add a verifiable parental consent step and keep the first name out of the URL.

Statements are limited to the package and the public documents named above.

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 Root level code analysis of the published application.

No Adherium servers or accounts were probed. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. REF HAILIE-2026-R1.