Security & Privacy Disclosure, Final Report

LinX CGM (com.microtech.aidexx.mgdl)

A glucose monitoring app that permits plaintext to a China-named host, and a privacy policy written for another country.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED

Target	LinX CGM (Micro Tech Medical (Hangzhou) Co., LTD per the Google Play developer field)
Notice / Publication	2026-08-21 / 2026-11-19 (90 days, unchanged)
Versions Audited	2.5.0 / 2501 (analysed 2026-08-21)
Findings	10: 6 High, 3 Medium, 1 Low (C1 to C3 reassessed from Critical, H1 from High to Medium, H5 from High to Low)
Status	NO REPLY OF ANY KIND AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`3c57694728938ae87ebb93aba09890f8db4a5f454142e62599b0861022255d01`

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 5

4 Architecture & Data Flow 6

5 Findings 7

5.1 C1: Five SDK providers from three vendors initialise before any consent screen, and the binary contains no consent management . . . 7

5.2 C2: The network security configuration permits cleartext HTTP to eleven hosts, including a China-named health platform host, three private LAN addresses and a log-upload entry, while the store label says data is encrypted in transit 8

5.3 C3: No privacy policy applicable to EU users was reachable, three company names appear, and no EU representative is named . . . 9

5.4 H1: Firebase API key, app ID, sender ID and Cloud Storage bucket name are hardcoded in the public APK . . . 10

5.5 H2: Three push services run in parallel, including Getui, and none is named in the reachable policy . . . 11

5.6 H3: Background location is requested next to a Bluetooth scan permission that declares no location use, and an internal string describes continuous collection 12

5.7 H4: Four Tencent SDK products are embedded and named nowhere in the reachable policy . . . 13

5.8 H5: A commercial app-shielding layer hides about 75 percent of the application from static inspection . . . 14

5.9 M1: No age check or parental consent flow in an app rated PEGI 3 that records health data . . . 14

5.10 M2: The Huawei routing configuration lists a mainland China endpoint among five candidates . . . 15

6 Impact Analysis 15

7 The Complete Chain 16

8 Data Protection: Article by Article 17

9 Consumer Protection & Platform Disclosures 18

10 Regulatory & Legal Landscape 18

11 What LinX Got Right 18

12 Indicators of Compromise & Reproducible Evidence 19

13 Disclosure Timeline & Outcome 20

14 Residual Risk & Recommendations 20

Executive Summary

LinX CGM is the Android companion app for a continuous glucose monitoring sensor. It pairs over Bluetooth, shows real-time blood glucose readings and records insulin dosage, medication, exercise and free-text disease fields. The package is com.microtech.aidexx.mgdl, version 2.5.0. The Google Play developer field names Micro Tech Medical (Hangzhou) Co., LTD.

On 21 August 2026 RFI-IRFOS sent a coordinated disclosure notice under REF LINXCGM-2026-R1 to linx.support@microtechmd.com and cs@microtechmd.com, copying sales@microtechmd.com, the Austrian Datenschutzbehörde and the European Data Protection Supervisor. It reported ten findings from a root level code analysis and asked three written questions. A follow-up on 12 September 2026 and a reminder on 17 October 2026 restated them. No reply of any kind is on record as of 14 November 2026.

The governing thesis is that an EU user of this app cannot tell who is responsible and what the rules are. No privacy policy applicable to EU users was reachable. The only readable policy belongs to a South African distributor and is written for South African law (C3). The release build permits cleartext HTTP to eleven hosts, including the controller's clinician platform at a China-named host, three private LAN addresses and a log-upload entry, while Google Play says data is encrypted in transit (C2). Components from Google, Huawei and Tencent initialise before any consent screen (C1), three push services and four Tencent SDK products are named in no reachable document (H2, H4), and background location is described differently in two languages (H3).

The report is specific about limits. No network traffic was captured, so the report shows what the build permits and not what a given phone sends. About 75 percent of the application logic is shielded and was not inspected (H5), so statements about what the app does not do are limited to the manifest, resources and native libraries. The strongest facts are the cleartext permission, the missing policy and the initialisation order, all read directly from files.

Scope: Root level code analysis of the Google Play release 2.5.0 (versionCode 2501) as obtained in the XAPK bundle: AndroidManifest.xml, resources, res/xml/network_security_config.xml, bundled assets and the 18 native libraries of the arm64-v8a split. The application logic inside assets/overdrive/overdrive.data (31.7 MB, shielded) was not inspected. Public web pages read by plain HTTP GET on 21 August 2026: the Google Play listing, microtechmd.com and linxcgm.co.za/privacy-policy. No backend was called, no account was created, no traffic was intercepted and no runtime instrumentation was used. Report prepared for the publication date. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89.

ID	Severity	Title
C1	HIGH	Five SDK providers from three vendors initialise before any consent screen, and the binary contains no consent management
C2	HIGH	The network security configuration permits cleartext HTTP to eleven hosts, including a China-named health platform host, three private LAN addresses and a log-upload entry, while the store label says data is encrypted in transit
C3	HIGH	No privacy policy applicable to EU users was reachable, three company names appear, and no EU representative is named
H1	MEDIUM	Firebase API key, app ID, sender ID and Cloud Storage bucket name are hardcoded in the public APK
H2	HIGH	Three push services run in parallel, including Getui, and none is named in the reachable policy
H3	HIGH	Background location is requested next to a Bluetooth scan permission that declares no location use, and an internal string describes continuous collection
H4	HIGH	Four Tencent SDK products are embedded and named nowhere in the reachable policy
H5	LOW	A commercial app-shielding layer hides about 75 percent of the application from static inspection
M1	MEDIUM	No age check or parental consent flow in an app rated PEGI 3 that records health data
M2	MEDIUM	The Huawei routing configuration lists a mainland China endpoint among five candidates

ID	Disclosed	This report	Status on 14 November 2026

Finding Status at a Glance

ID	Disclosed	This report	Status on 14 November 2026
C1	CRITICAL	HIGH	No reply. Reassessed: initialisation order is shown, transmission is not.
C2	CRITICAL	HIGH	No reply. Reassessed: plaintext is permitted, its use is not shown.
C3	CRITICAL	HIGH	No reply. Reassessed: transparency defect with no exploit path.
H1	HIGH	MEDIUM	No reply. Reassessed: restrictions on the key are not known.
H2	HIGH	HIGH	No reply.
H3	HIGH	HIGH	No reply.
H4	HIGH	HIGH	No reply.
H5	HIGH	LOW	No reply. Reassessed: an evidence limit, not a data flow.
M1	MEDIUM	MEDIUM	No reply.
M2	MEDIUM	MEDIUM	No reply.

Subject & Operator Analysis

Three names appear across the product surfaces. Google Play lists Micro Tech Medical (Hangzhou) Co., LTD as developer. The corporate site microtechmd.com signs its footer MicroTech Medical, Inc. and carries a Zhejiang ICP registration, which indicates a company registered in the People's Republic of China. The distributor Homemed (Pty) Ltd of Pretoria, South Africa operates linxcgm.co.za, whose privacy policy cites the manufacturer and the Pancares platform as references.

Pancares is the manufacturer's clinician-facing remote-monitoring platform. The app ships a dedicated "Share with Pancares Account" setting, and the platform's own public description says it lets doctors and nurses view blood glucose data in real time. The network security configuration lists five pancares.com hostnames, one of them china.pancares.com.

No EU representative, data protection officer or direct contact e-mail address appears in the binary, on the corporate site or in the distributor policy. The corporate site offers a web contact form. Which company is the controller is not established by the material and is the first question put to the operator.

Architecture & Data Flow

The distributed classes.dex is a bootstrap stub of 5,632 bytes. The application and component factory classes belong to a commercial shielding product, and the logic sits in a 31.7 MB opaque payload loaded at start. The manifest, resources, network security configuration, assets and 18 native libraries are not shielded and were inspected in full.

Data flow as the client shows it: the app pairs with the sensor over Bluetooth, which needs location permissions on older Android versions. Push notifications run through Getui, Huawei HMS and Firebase. Crash and performance tooling comes from Tencent. Firebase and Huawei AGConnect initialise at start. Clinician sharing runs through Pancares hosts, and the network security configuration permits plaintext to all of them.

What the client does not show: what is sent to each service, what the shielded logic does, and which Huawei endpoint is selected. These are outside the analysis and no claim is made about them.

Findings

C1: Five SDK providers from three vendors initialise before any consent screen, and the binary contains no consent management

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 21 August 2026, reassessed in this report

Five ContentProviders are declared: Google ML Kit (initOrder 99), Firebase (initOrder 100, directBootAware true), the Huawei ML SDK initialiser, Huawei AGConnect, and the Tencent RMonitor launch installer. Component discovery services for Firebase, ML Kit and Huawei AGConnect start further components. Android instantiates providers during application creation, before any Activity, so no in-app agreement screen can run first. Two Firebase components are also directBootAware and can start before device unlock. A string search of the decompiled resources for onetrust, didomi, usercentrics, consentmanager, iabtcf and cmpsdk returned zero matches. The only consent-adjacent texts are a first-run agreement checkbox (user_sign_agreement) and a later ”Privacy Agreement Update” prompt (version_policy_update_title), both rendered inside an Activity. Because about 75 percent of the application logic ships in a shielded payload (H5), consent code inside that payload cannot be excluded by this analysis, but the providers above run before that payload can show any screen. RFI-IRFOS blast-radius escalation: raised from MEDIUM to HIGH because the app processes real-time glucose, insulin and medication data, the initialisation order is demonstrated from the manifest, and it spans three vendor stacks in two jurisdictions at once with no consent gate in the binary. Transmission of any health field was not observed, which keeps the finding below Critical.

```
<provider android:authorities="com.microtech.aidexx.mgdl.mlkitinitprovider"
    android:exported="false" android:initOrder="99"
    android:name="com.google.mlkit.common.internal.MlKitInitProvider"/>
<provider android:authorities="com.microtech.aidexx.mgdl.firebaseinitprovider"
    android:directBootAware="true" android:exported="false" android:initOrder="100"
    android:name="com.google.firebase.provider.FirebaseInitProvider"/>
<provider android:authorities="com.microtech.aidexx.mgdl.MLInitializerProvider"
    android:exported="false"
    android:name="com.huawei.hms.mlsdk.common.provider.MLInitializerProvider"/>
<provider android:authorities="com.microtech.aidexx.mgdl.AGCInitializeProvider"
    android:exported="false"
    android:name="com.huawei.agconnect.core.provider.AGConnectInitializeProvider"/>
<provider android:authorities="com.microtech.aidexx.mgdl.rmonitor-installer"
    android:exported="false"
    android:name="com.tencent.rmonitor.launch.AppLaunchMonitorInstaller"/>
```

Disclosed as CRITICAL on 21 August 2026. This report counts the five ContentProviders shown above, where the notice counted six components in total.

Impact: A person who installs the app to see their glucose readings has components from Google, Huawei and Tencent starting up on every launch, before they have seen or accepted anything, and a person who installs it and never opens the agreement screen is covered too.

Fix: Disable automatic initialisation for each vendor SDK in the manifest, start them from

application code after a recorded consent, and document the Art. 6(1) basis for anything that must run earlier.

C2: The network security configuration permits cleartext HTTP to eleven hosts, including a China-named health platform host, three private LAN addresses and a log-upload entry, while the store label says data is encrypted in transit

---

MEDIUM, CVSS v4.0 AV:A/AC:L/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 21 August 2026, reassessed in this report

res/xml/network_security_config.xml sets cleartextTrafficPermitted to true in every domain-config. The hosts are china.pancares.com, gateway.pancares.com, linx-h5.pancares.com, dev-linx-h5.pancares.com and xagpwebforeign.pancares.com, and six bare IP addresses. Three of the IP addresses are in RFC 1918 private space (192.168.222.26, 192.168.226.5, 192.168.224.150) and read as development or staging leftovers. The other three (212.41.10.132, 212.41.10.133, 35.179.178.176) are outside private ranges and their operator was not determined. A separate entry names the path china.pancares.com/backend/vcs/log/uploadLog. The Android network security configuration matches hostnames and not paths, so that entry adds no extra host and is covered by the china.pancares.com entry above it. Two of the entries restrict trust to bundled certificates (raw resources pancares_com and china_pancares_com). A debug-overrides block trusting user-installed certificate authorities is also present in the release file and is inert unless the build is debuggable. The manifest also sets usesCleartextTraffic to true, which Android ignores for hostnames covered by a network security configuration on API level 24 and above, so the per-host entries are the operative permission. Google Play Data Safety, read on 21 August 2026, states ”Data is encrypted in transit.” and lists only ”Device or other IDs” as shared with third parties. The app ships a ”Share with Pancares Account” setting (permission_pancares), and Pancares is the controller’s clinician-facing platform. RFI-IRFOS blast-radius escalation: raised from MEDIUM to HIGH because the hosts include the controller’s own clinician remote-monitoring platform that receives glucose and insulin data, the permission sits in the release build, and it contradicts a public statement made to every prospective user. Runtime use of plaintext was not observed, which keeps the finding below Critical.

```
<domain-config cleartextTrafficPermitted="true">
    <domain includeSubdomains="true">china.pancares.com</domain>
    <domain includeSubdomains="true">gateway.pancares.com</domain>
    <domain includeSubdomains="true">212.41.10.133</domain>
    <trust-anchors><certificates src="@raw/pancares_com" /></trust-anchors>
</domain-config>
<domain-config cleartextTrafficPermitted="true">
    <domain includeSubdomains="false">china.pancares.com/backend/vcs/log/uploadLog</
    domain>
    <trust-anchors><certificates src="@raw/china_pancares_com" /></trust-anchors>
</domain-config>
... further entries, same attribute:
212.41.10.132  linx-h5.pancares.com  dev-linx-h5.pancares.com
192.168.222.26  192.168.226.5  xagpwebforeign.pancares.com
192.168.224.150  35.179.178.176
```

Host class	Count	Hosts
pancares.com host-names	5	china, gateway, linx-h5, dev-linx-h5, xagpweb-foreign
Private RFC 1918 ad-dresses	3	192.168.222.26, 192.168.226.5, 192.168.224.150
Other bare IP addresses	3	212.41.10.132, 212.41.10.133, 35.179.178.176

Disclosed as CRITICAL on 21 August 2026. The R1 notice counted five hardcoded internal IP addresses. The file contains six bare IP addresses, three of them private. The vector uses AV:A and AT:P because exploitation needs a position on the network path and a request that actually uses plaintext, which the static analysis shows is permitted and does not show is used.

Impact: A person using the app on public Wi-Fi may have glucose, insulin and log data sent without transport encryption to a host the controller itself operates, while the store page tells them the opposite.

Fix: Remove cleartextTrafficPermitted from every production domain-config, delete the staging and private addresses and the debug-overrides block from the release file, and correct the Data Safety statement to match the shipped behaviour.

C3: No privacy policy applicable to EU users was reachable, three company names appear, and no EU representative is named

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 21 August 2026, reassessed in this report

No privacy policy URL is present in res/values/strings.xml, res/values/public.xml or resources.arsc. The label about_privatePolicy exists but its target is not statically present, which is consistent with the shielded payload (H5). No contact e-mail address appears in the decompiled resources. The only company identifiers in the resources are the bare domains www.microtechmd.com and microtechmd.com. The Google Play developer field reads Micro Tech Medical (Hangzhou) Co., LTD. The corporate site microtechmd.com signs its footer MicroTech Medical, Inc., carries a Zhejiang ICP registration, and offers a web contact form and no e-mail address, EU representative or data protection officer. The only privacy policy located and read, linxcgm.co.za/privacy-policy, belongs to Homemed (Pty) Ltd of Pretoria, South Africa, a distributor. It is written against the South African Protection of Personal Information Act, never mentions the GDPR or the EU, and states that it applies to all users. A policy object referenced from controller infrastructure on a cloudfront.net host returned 403 AccessDenied when fetched. The Play Data Safety section lists health and fitness data as collected and not as shared, while the app ships a ”Share with Pancares Account” feature that lets external clinicians view a patient’s data according to the platform’s own public description. Whether the three names are related legal entities was not verified against a company register. RFI-IRFOS blast-radius escalation: raised from MEDIUM to HIGH because the data is Art. 9 health data, the only readable policy is written for another country, and an EU resident has no document and no contact in the EU that explains their rights. The finding is a transparency and accountability defect with no technical exploit path, which is why it is rated below Critical.

```
about_privatePolicy      (label only, no URL in any resource)
appInfo_company_url      www.microtechmd.com
appInfo_instructions_url microtechmd.com
permission_pancares      "Share with Pancares Account" feature text
```

Surface	Name given	Read on
Google Play developer field	Micro Tech Medical (Hangzhou) Co., LTD	2026-08-21
Corporate site footer	MicroTech Medical, Inc.	2026-08-21
Only readable policy, linx-cgm.co.za	Homemed (Pty) Ltd, Pretoria, POPIA only	2026-08-21
Policy object on a cloud-front.net host	HTTP 403 AccessDenied	2026-08-21

Disclosed as CRITICAL on 21 August 2026. The R1 notice also named a fourth company for a different product. That statement rests on a page not documented in the analysis file for this report and is not repeated here.

Impact: An Austrian user who wants to know who holds their glucose history, or to ask for its deletion, finds no policy written for them and no one in the EU to ask.

Fix: Publish one controller identity and a policy that addresses EU data subjects under the GDPR, name an Art. 27 representative with an EU address and a data protection contact, link the policy inside the app, and list the clinician sharing feature in the store disclosure.

H1: Firebase API key, app ID, sender ID and Cloud Storage bucket name are hardcoded in the public APK

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 21 August 2026, reassessed in this report

res/values/strings.xml carries gcm_defaultSenderId, google_api_key, google_app_id, google_storage_bucket and project_id for the Firebase project wtyl-5d701. The project ID does not match the product or the company name and reads as an internal codename. Google documents Firebase API keys as identifiers and not secrets, so this is a resilience question and not a secrecy one. No request was made against the key or the bucket, so the quota restrictions, the Storage security rules and the presence of App Check are not known. The key is abbreviated here and is available in the public APK.

```
<string name="gcm_defaultSenderId">956972018206</string>
<string name="google_api_key">AIzaSyCmg8H-q9pbE2QSozc2G36CDUNEWUa7234</string>
<string name="project_id">wtyl-5d701</string>
<string name="google_storage_bucket">wtyl-5d701.firebasestorage.app</string>
```

Disclosed as HIGH on 21 August 2026. This report rates the finding Medium. The vector uses AT:P because the effect depends on missing restrictions that the analysis did not test.

Impact: If the key or the bucket rules are loose, someone else can use up the quota the app relies on, or read or write files in a store attached to a diabetes app.

Fix: Restrict the key by application signature and API, confirm Storage rules deny by default, enable App Check and keep the key per service.

H2: Three push services run in parallel, including Getui, and none is named in the reachable policy

---

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)

The manifest integrates the com.igexin.sdk namespace (Getui, a Beijing-based push provider) with its own process (:pushservice), services, activities and a hardcoded PUSH_APPID. In parallel the app uses Google Firebase Cloud Messaging and the Huawei HMS and AGConnect push infrastructure. A single push channel would be functionally sufficient. The reachable policy (C3) names none of the three vendors and no transfer mechanism. What identifiers the Getui SDK transmits was not observed. RFI-IRFOS blast-radius escalation: raised from MEDIUM to HIGH because the app drives low-glucose alerts, three independent processors receive device and notification identifiers for that one purpose, one of them under Chinese jurisdiction, and no reachable document names any of them or any transfer safeguard.

```
<service android:name="com.microtech.aidexx.service.push.GeTuiIntentService"/>
<service android:exported="false" android:name="com.igexin.sdk.FcmPushService">
  <intent-filter><action android:name="com.google.firebase.MESSAGING_EVENT"/></intent-
    filter>
</service>
<service android:name="com.igexin.sdk.FcmPushIntentService"
    android:permission="android.permission.BIND_JOB_SERVICE" android:process=":
    pushservice"/>
<meta-data android:name="PUSH_APPID" android:value="K9FMnzHPkl7TjcpssIzxV6"/>
```

Impact: A person with diabetes who switches on low-glucose alerts has their device identifiers passed to three push providers, one in China, none of which they are told about.

Fix: Reduce the app to one push channel per platform, name each push provider and its role in the policy, and document the transfer basis for any provider outside the EU.

H3: Background location is requested next to a Bluetooth scan permission that declares no location use, and an internal string describes continuous collection

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.8 (CVSS-B)

The manifest declares BLUETOOTH_SCAN with usesPermissionFlags neverForLocation and also ACCESS_BACKGROUND_LOCATION, ACCESS_FINE_LOCATION and ACCESS_COARSE_LOCATION. The user-facing string permission_location_desc says "Turn on localization to use Bluetooth functionality for CGM connection." A second string for the same permission, permission_location_desc_real, is written in Chinese and translates as: the app collects location data, even when the application is in the background, in order to receive CGM data in real time. Fine or coarse location is explicable for the minSdk 24 range, because Android 11 and earlier require a location permission for Bluetooth scanning. The finding concerns the background tier and the difference between the two descriptions. Whether the background tier is technically required for the app's background scanning on Android 10 and 11 was not tested. RFI-IRFOS blast-radius escalation: raised from MEDIUM to HIGH because the developer's own internal string states that location data is collected even when the app is in the background, the user-facing English string describes only Bluetooth, and the data is the location trail of people managing a chronic condition.

```
<uses-permission android:name="android.permission.BLUETOOTH_SCAN"
    android:usesPermissionFlags="neverForLocation"/>
<uses-permission android:name="android.permission.ACCESS_BACKGROUND_LOCATION"/>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
permission_location_desc       Turn on localization to use Bluetooth functionality for
     CGM connection.
permission_location_desc_real  (Chinese text, translation given in the finding)
```

The vector uses AV:L and UI:P because the user must grant each location permission at runtime.

Impact: A person who agrees to the Bluetooth explanation also hands over a background location trail that the English text does not describe.

Fix: Request background location only where a documented feature needs it, show one accurate description in every language, and publish the purpose in the policy.

H4: Four Tencent SDK products are embedded and named nowhere in the reachable policy

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)

The arm64-v8a native library split contains libBugly_Native.so, libbugly_dumper.so, libbuglybacktrace.so (Tencent Bugly crash reporting), libmarsxlog.so (Tencent Mars xlog logging) and libmmkv.so (Tencent MMKV key-value storage). The manifest declares the RMonitor launch installer provider (C1). Bugly is built to transmit stack traces and device state on a crash. The reachable policy and the Play Data Safety sharing category name none of the four products. What a crash report from this app contains was not observed. RFI-IRFOS blast-radius escalation: raised from MEDIUM to HIGH because crash and performance tooling in a glucose app can carry device state at the moment of a failure to a Chinese-jurisdiction processor, and no reachable document names the processor or a transfer safeguard.

```
libBugly_Native.so      211,856 bytes   Tencent Bugly crash reporting
libbugly_dumper.so      113,808 bytes   Tencent Bugly crash dumper
libbuglybacktrace.so    838,968 bytes   Tencent Bugly backtrace
libmarsxlog.so          657,968 bytes   Tencent Mars xlog logging
libmmkv.so              597,000 bytes   Tencent MMKV storage
com.tencent.rmonitor.launch.AppLaunchMonitorInstaller  (provider)
```

Impact: When the app crashes on the phone of a person with diabetes, a crash report may go to a Tencent-operated service that the policy does not mention.

Fix: Name each Tencent component and its role in the policy, document the transfer basis, or replace the components with tooling in the EU.

H5: A commercial app-shielding layer hides about 75 percent of the application from static inspection

LOW, CVSS v4.0 AV:L/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.1 (CVSS-B), disclosed as HIGH on 21 August 2026, reassessed in this report

The manifest names com.mobile.overdrive.RevolutApplication and com.mobile.overdrive.RevolutComponentFactory as the Application and AppComponentFactory. classes.dex is 5,632 bytes. The business logic ships in assets/overdrive/overdrive.data, 31,728,784 bytes with no recognisable file signature, about 75 percent of the base APK by uncompressed size. The brand token Revolut inside a glucose app has no visible connection to the app or the manufacturer and most plausibly comes from a template of the shielding product. No link to any company of that name is asserted. Code shielding is a legitimate anti-tampering measure and is not itself a data protection breach. It is recorded because it sets the limit of this analysis: the manifest, resources and native libraries were fully inspected, and the logic that uses them was not.

```
android:appComponentFactory="com.mobile.overdrive.RevolutComponentFactory"
android:name="com.mobile.overdrive.RevolutApplication"
classes.dex                        5,632 bytes
assets/overdrive/overdrive.data    31,728,784 bytes
```

Disclosed as HIGH on 21 August 2026. This report rates the finding Low. It limits what can be shown about the app and does not by itself expose anyone to harm.

Impact: The controller, and not an outside reviewer, has to be the one who can show what the hidden code does with glucose data.

Fix: State in writing how the shielded logic uses the permissions and endpoints listed in this report, or provide an unshielded build to a supervisory authority on request.

M1: No age check or parental consent flow in an app rated PEGI 3 that records health data

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)

A search of the string resources for age, birthdate, underage, minor and parental terms returned only a generic profile string showing a number of years. No birthdate field, minimum-age check or parental consent flow appears in the resources. Google Play lists the content rating as PEGI 3 (Everyone) on 21 August 2026. Type 1 diabetes is often diagnosed in childhood, so younger users are a foreseeable group. Logic inside the shielded payload (H5) is outside this analysis.

The finding is limited to what the resources show. It does not state that the app is directed at children.

Impact: A child or young teenager can use the app with no age check and no parental involvement, although the data is health data.

Fix: Add an age assurance step with parental consent where the national age of digital consent applies, and assess paediatric use in a data protection impact assessment.

M2: The Huawei routing configuration lists a mainland China endpoint among five candidates

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)

assets/grs_sdk_server_config.json lists five candidate base URLs for the Huawei Global Routing Service: grs.dbankcloud.com, grs.dbankcloud.cn, grs.dbankcloud.asia, grs.platform.dbankcloud.ru and grs.dbankcloud.eu. Which endpoint a device in the EU selects at runtime is UNVERIFIED, because that needs network capture and none was made. The finding is limited to the presence of the .cn option in the shipped file.

```
"grs_base_url": [
  "https://grs.dbankcloud.com",
  "https://grs.dbankcloud.cn",
  "https://grs.dbankcloud.asia",
  "https://grs.platform.dbankcloud.ru",
  "https://grs.dbankcloud.eu"
]
```

The vector uses AT:P and AC:H because the effect depends on a runtime routing choice that was not observed.

Impact: If a device is routed to the China endpoint, requests from an EU phone reach infrastructure under Chinese jurisdiction without the user being told.

Fix: Pin EU device routing to the EU endpoint, remove unused regional candidates and document which Huawei services receive which data.

Impact Analysis

People affected: users of the LinX sensor who log glucose, insulin, medication and exercise, which is health data in the sense of Art. 9 GDPR by any reading, and who include children and teenagers because no age check exists.

- Three vendor stacks start before consent (C1), and plaintext is permitted to the controller's own health platform (C2).
- No policy applies to EU users and no one in the EU can be asked (C3).
- Hardcoded identifiers (H1) and three push services (H2) widen the set of parties around the data.
- Background location is described differently by language (H3), and Tencent tooling is named nowhere (H4).
- The shielded payload limits what any outside party can verify (H5), and no age assurance exists (M1).

The ratings stay conservative. The analysis does not show what is transmitted in any of these cases, and the build keeps several protections, listed below.

The Complete Chain

Step 1, install and first launch: Google, Huawei and Tencent providers start during application creation, before the in-app agreement can appear (C1).

Step 2, policy: the user looks for a privacy policy. The app contains no link, the manufacturer's site has none that was found, and the only readable policy is a South African one (C3).

Step 3, pairing: the sensor connects over Bluetooth. Background location is requested next to a scan permission that declares no location use (H3).

Step 4, alerts and diagnostics: three push services and Tencent crash and performance tooling run in the app (H2, H4).

Step 5, clinician sharing: the user enables sharing with a Pancares account. The release build permits plaintext to Pancares hosts and to private and bare IP addresses, and the store page says data is encrypted in transit (C2).

Step 6, the person tries to act: no EU representative, no data protection officer and no contact e-mail address is named anywhere reachable (C3).

Article	Engaged by	Finding

Data Protection: Article by Article

Article	Engaged by	Finding
Art. 3(2)	The policy claims to cover all users, offering to people in the Union	C3
Art. 5(1)(a)	Store statements that differ from the shipped build, no applicable policy	C2, C3
Art. 5(1)(c)	Three push services, background location	H2, H3
Art. 5(2)	Controller must demonstrate compliance, shielded logic	C1, C2, H5
Art. 6(1), Art. 7(1)	Providers start before any consent mechanism	C1
Art. 8	No age assurance	M1
Art. 12(1)	No intelligible policy for EU users	C3
Art. 13, Art. 14	Recipients, transfers and contact not provided	C3, H2, H4
Art. 13(1)(e)	Push and Tencent processors not named	H2, H4
Art. 25	Defaults and design	C1, H1, H3
Art. 27	No EU representative	C3
Art. 32(1)(a)(b)	Cleartext permitted to health hosts, key restrictions unknown	C2, H1
Art. 35	Paediatric use in an impact assessment	M1
Art. 44, Art. 46	Transfers to China-jurisdiction processors and endpoints	C2, H2, H4, M2

Art. 27(2)(a) exempts only processing that is occasional, does not include large-scale processing of special categories, and is unlikely to risk individuals' rights. A glucose monitoring service processes health data as its core function. Whether the processing here is large scale is a question for the controller and the supervisory authority.

Consumer Protection & Platform Disclosures

Google Play Data Safety states that data is encrypted in transit and lists only device or other identifiers as shared. The shipped network security configuration permits cleartext to eleven hosts (C2), and the app contains a clinician sharing feature for health data (C3). The content rating of PEGI 3 sits beside a health product with no age check (M1). RFI-IRFOS makes no determination about the platform's own developer rules and records the differences between the controller's statements and its build.

Regulatory & Legal Landscape

Competent authority: no EU main establishment is identified, so the one-stop-shop mechanism does not apply and each concerned authority is competent. For a matter initiated from Austria the Österreichische Datenschutzbehörde is the authority, with the European Data Protection Supervisor copied on the notice.

Pre-consent initialisation also engages Art. 5(3) of Directive 2002/58/EC as implemented in Austria by § 165(3) TKG 2021.

Medical device context: if the software is placed on the EU market as part of a continuous glucose monitoring system, Regulation (EU) 2017/745 on medical devices may apply to it, with its own requirements for cybersecurity and information. CE marking and conformity status were not examined and are UNVERIFIED. No finding in this report depends on them.

Comparison within the programme: pre-consent initialisation is a recurring pattern. This case differs in the number of jurisdictions in one stack and in the absence of any policy written for EU users.

What LinX Got Right

- BLUETOOTH_SCAN carries the neverForLocation flag, the correct way to declare Bluetooth scanning without a location use.
- Custom trust anchors are bundled for the two main Pancares entries, which restricts trust for those hosts, even though cleartext is permitted beside them.
- allowBackup is false, which blocks backup extraction of local glucose records.
- targetSdkVersion is 35 and the granular Bluetooth permissions of Android 12 and later are used.
- The app ships a fallback for devices without Google Play services.
- The in-app clinical reference text cites peer-reviewed literature for its Glucose Management Indicator explanation.

Indicators of Compromise & Reproducible Evidence

Every point below is reproducible by another researcher from the public Google Play release and the public web pages named.

```
Package        com.microtech.aidexx.mgdl
Version        2.5.0 (versionCode 2501, built 27 April 2026)
Sdk            minSdk 24, targetSdk 35
Bundle         XAPK 44.8 MB, base APK 20.1 MB, arm64-v8a split 21.5 MB

XAPK SHA-256
4a105504901d2eefae896bd01ba2b9e64f417521067718e793625be85d7a6713

base APK SHA-256
3c57694728938ae87ebb93aba09890f8db4a5f454142e62599b0861022255d01
```

```
Firebase       project_id wtyl-5d701
Bucket         wtyl-5d701.firebasestorage.app
Getui          com.igexin.sdk, PUSH_APPID K9FMnzHPkl7TjcpssIzxV6
Shield         com.mobile.overdrive.RevolutApplication
Hosts          china.pancares.com  gateway.pancares.com  linx-h5.pancares.com
               dev-linx-h5.pancares.com  xagpwebforeign.pancares.com
Bare IPs       212.41.10.132  212.41.10.133  35.179.178.176
Private IPs    192.168.222.26  192.168.226.5  192.168.224.150
```

```
play.google.com/store/apps/details?id=com.microtech.aidexx.mgdl   Data Safety, PEGI 3
microtechmd.com                          footer MicroTech Medical, Inc.
linxcgm.co.za/privacy-policy             Homemed (Pty) Ltd, POPIA only
cloudfront.net policy object             HTTP 403 AccessDenied
```

Chain of custody: the package was not present on the RFI-IRFOS test device. The XAPK was downloaded from APKPure after the version and developer name were cross-checked against the live Google Play listing. The signing certificate SHA-1 (1a40bd0bc6a1faac52ca3f8cd1bafc49f2a85276) is taken from the APKPure security report for the arm64-v8a variant and was not independently verified. No backend was contacted.

Disclosure Timeline & Outcome

2026-08-21 First notice (REF LINXCGM-2026-R1) to linx.support@microtechmd.com and cs@microtechmd.com, CC sales@microtechmd.com, the Austrian Datenschutzbehörde and the European Data Protection Supervisor. Findings C1, C2, C3 stated in full, five further findings summarised, three questions asked.

2026-09-12 Follow-up to the same addresses with the findings unchanged, 22 days after the first notice.

2026-10-17 Reminder from security@rfi-irfos.com, 33 days before publication.

2026-11-14 No reply of any kind on record.

2026-11-19 Publication date, unchanged since 21 August 2026 and independent of any reply.

Residual Risk & Recommendations

Open on the evidence of this report: all ten findings. No answer to any question is on record. The findings describe version 2.5.0 as analysed on 21 August 2026. The state of later builds is not part of this report.

For the operator, in order of effect: remove cleartext permission and the staging and private addresses from the release configuration and correct the store statement (C2), publish a policy for EU data subjects with a named controller, an Art. 27 representative and a contact (C3), gate vendor SDK initialisation behind a recorded consent (C1), reduce to one push channel and name each push and crash processor (H2, H4), align the location descriptions and request background location only where needed (H3), restrict the Firebase key and confirm Storage rules (H1), pin routing to the EU endpoint (M2), add age assurance (M1), and explain the shielded logic to a supervisory authority on request (H5).

For users: review the location permission you granted and whether sharing with a Pancares account is switched on, avoid public Wi-Fi while the plaintext permission stands, and contact the operator in writing with an access request if you want to know which entity holds your data.

Questions that remain open and are not answered by the client: whether plaintext is used at runtime, what the shielded payload does, which Huawei endpoint is selected and how the three named companies relate.

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 root level code analysis of the published application using publicly available tooling, plus public web pages read by plain HTTP GET. No 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 LINXCGM-2026-R1.