# Security & Privacy Disclosure, Final Report

## My i-Limb for Android (com.ossur.myilimb.app)

A hand prosthesis control app that ships real AWS identifiers, legacy test code and empty backup rules, and a vendor that answered the three questions in writing.

**PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. EMBARGO 21 NOVEMBER 2026. SUBSTANTIVE VENDOR REPLY RECEIVED 17 SEPTEMBER 2026, NO REPLY TO THE MAILS OF 17 OCTOBER AND 15 NOVEMBER 2026.**

| | |
|---|---|
| **Target** | Össur Europe B.V., Eindhoven (group: Össur hf, Embla Medical) |
| **Versions Audited** | 1.0.16 / 130 (analysis 2026-08-22) |
| **Notice / Publication** | 2026-08-23 / 2026-11-21 (90 days) |
| **Findings** | 4: 3 Medium, 1 Low (C1 reassessed from Critical, H1 and H2 from High, H1 held at Medium by blast-radius escalation) |
| **Status** | SUBSTANTIVE REPLY RECEIVED 17 SEPTEMBER 2026 (follow-up answer 18 September 2026). NO REPLY TO THE MAILS OF 17 OCTOBER AND 15 NOVEMBER 2026 AS OF 21 NOVEMBER 2026. |
| **SHA-256 (base APK)** | `02d488c5fa23fa49151438a613cc2efc66345bb7043325d55f928a2720aae699` |

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 Vendor Reply of 17 and 18 September 2026 5

4 Subject & Operator Analysis 6

5 Architecture & Data Flow 7

6 Findings 8

6.1 C1: A real AWS account ID and SQS queue URL are hardcoded in the shipped app, next to repository classes for hand-specific commands and records . . . 8

6.2 H1: Legacy engineering, test and CAN-bus command classes ship in the patient-facing app, behind a device-level authorisation concept . . . . . 10

6.3 H2: allowBackup is true and both backup rule files are empty, so no exclusion is configured for the app's data . . . . . 12

6.4 M1: No network security configuration and no certificate pinning . . . . . 13

7 Impact Analysis 13

8 The Complete Chain 14

9 Inference Data and Control Data 14

10 Observation: PEGI 3 Rating on a Medical App 15

11 Data Protection: Article by Article 15

12 Regulatory & Legal Landscape 15

13 Indicators of Compromise & Reproducible Evidence 16

14 Disclosure Timeline & Outcome 17

15 What Össur Got Right 18

16 Residual Risk & Recommendations 18

## Executive Summary

My i-Limb is the Bluetooth control app for the myoelectric hands and fingers i-Limb Quantum, i-Limb Ultra, i-Limb Access, i-Digits Quantum and i-Digits Access, published on Google Play by Össur Europe B.V. in Eindhoven. On 23 August 2026 RFI-IRFOS sent four findings from a root level code analysis of version 1.0.16 under REF SSURILIMB-2026-R1. The package namespace shows the Touch Bionics codebase carried forward under the Össur storefront.

The main finding was a real AWS account ID and SQS queue URL in plaintext in the shipped app, next to repository classes for hand-specific commands and records. Further findings covered a legacy engineering, test and CAN-bus command layer in the patient build, empty backup rules with allowBackup set to true, and missing certificate pinning. No AWS resource was contacted, no device was paired and no command was sent.

The vendor answered in writing on 17 September 2026. It stated that grip submissions are reviewed by staff before others can use them, that the identifiers alone grant no access and that additional access restrictions were applied. It stated that the CAN class is inactive, the test code is stubs and the authorisation check runs in the prosthesis firmware. It stated that the two databases named in the notice are non-functional and that the Android app records no EMG data, and it confirmed that no backup exclusion rules exist. This report records the statements as the vendor's answer and rates accordingly.

Three of the four severities sent in the first notice are lower in this report. The open items are the backup rules, the removal of the test code and further AWS improvements. The vendor stated on 18 September 2026 that it does not give release windows. RFI-IRFOS asked for the shipped version of each item on 17 October 2026 and again on 15 November 2026, 6 days before publication, and has received no reply to either mail as of 21 November 2026. RFI-IRFOS has no confirmation of these items in a shipped build.

**Scope:** Root level code analysis of the Google Play release 1.0.16 (versionCode 130) as an XAPK obtained through a mirror and cross-checked against the live listing: manifest and resources through apktool, and class name, endpoint and secret searches over classes.dex. No Össur server or AWS resource was contacted, no device was paired and no command was sent. Dynamic analysis is not part of this report.

| ID | Severity | Title |
|---|---|---|
| C1 | MEDIUM | A real AWS account ID and SQS queue URL are hardcoded in the shipped app, next to repository classes for hand-specific commands and records |
| H1 | MEDIUM | Legacy engineering, test and CAN-bus command classes ship in the patient-facing app, behind a device-level authorisation concept |
| H2 | LOW | allowBackup is true and both backup rule files are empty, so no exclusion is configured for the app's data |
| M1 | MEDIUM | No network security configuration and no certificate pinning |

## Finding Status at a Glance

The table shows the severity sent in the first notice of 23 August 2026 next to the severity in this report. Three of the four severities are lower here. The reasons are the vendor's written answers of 17 September 2026 and the lower band that the evidence supports. The vendor answers are recorded as statements of the vendor. They were not verified against a newer build, and this report describes version 1.0.16 only.

| ID | Sent 23 Aug 2026 | This report | Basis |
|---|---|---|---|
| C1 | CRITICAL | MEDIUM | CVSS 6.3 for exposed cloud resource identifiers. Vendor states no access by identifier alone, staff review of submissions, access restrictions applied. |
| H1 | HIGH | MEDIUM | CVSS 2.3, raised one band by blast-radius escalation. Class inventory confirmed in the build. Vendor states the CAN class is inactive, test code is stubs, and authorisation is enforced in the firmware at connection. |
| H2 | HIGH | LOW | CVSS 1.0. Backup rules confirmed empty. Vendor states the two named databases are non-functional and that no EMG data is recorded. |
| M1 | MEDIUM | MEDIUM | CVSS 6.3. Not addressed in the reply. |

## Vendor Reply of 17 and 18 September 2026

The first notice went to the Play Store contact address of the publisher. The vendor wrote that this address was not part of its security intake, that the report reached its security organisation on 13 September 2026, and that reports to this address are now routed to the security team. The security officer of Embla Medical, the group of Össur, answered in writing on 17 September 2026. The reply addresses the three questions of the notice.

| Question | Vendor statement | Effect on this report |
|---|---|---|
| 1 AWS channel | The queue supports the grip-sharing feature. Staff review each grip before others can use it. Account ID and URL alone do not grant access. Configuration reviewed, additional access restrictions applied, further improvements under evaluation. | C1 reassessed from Critical to Medium. Access policy still not verified by RFI-IRFOS. |
| 2 Command surface | The CAN-related class belongs to unreleased devices and is not active. Test code is stubs and limited connection tests, removal planned for a future release. Authorisation is checked in the firmware when a connection is established and gates the whole command interface. Bluetooth proximity is required. | H1 reassessed from High to Medium. Class inventory confirmed in the shipped build. Stub removal and firmware coverage remain the vendor’s statement. |
| 3 Local data and backup | RecordingDatabase and AllCountsDatabase are non-functional carry-overs without operative code. The Android app does not record EMG data. No backup exclusion rules are defined and a restriction is under engineering review. | Muscle-signal claim removed from H2. Backup finding confirmed. H2 reassessed from High to Low. |

On 18 September 2026 RFI-IRFOS asked for a target version for each of three open items, namely the backup exclusion rules, the removal of the stub test code and the further AWS channel improvements. The vendor answered the same day that it does not communicate target versions or release windows externally and that changes appear in shipped builds as each completes development and testing. A further mail of 17 October 2026 asked for the version number per item. A mail of 15 November 2026 repeated the three items, corrected the publication date to 21 November 2026 and set out the reassessed severities. Neither mail

has been answered as of 21 November 2026.

## Subject & Operator Analysis

My i-Limb is the Bluetooth control app for the myoelectric hand prostheses i-Limb Quantum, i-Limb Ultra, i-Limb Access, i-Digits Quantum and i-Digits Access. It is published on Google Play by Össur Europe B.V., De Schakel 70, 5651 GH Eindhoven, Netherlands, with the developer contact playstore_agent@ossur.com. The in-app copyright string names Ossur hf for the years 2013 to 2025, and the internal package namespace com.touchbionics.myilimb confirms the Touch Bionics codebase carried forward under the Össur storefront. The vendor's reply came from the security officer of Embla Medical (thbaldursson@emblamedical.com). The Play listing shows the category Medical and the content rating PEGI 3 (Everyone). The app-specific privacy policy linked from the listing is https://www.ossur.com/global/privacy-policy.

| Item | Value |
|---|---|
| Package | com.ossur.myilimb.app |
| Internal namespace | com.touchbionics.myilimb.* |
| Version | 1.0.16 (versionCode 130) |
| XAPK SHA-256 | 7b0072f4245244a8525ed2d7ca9119537041110b14df2ae6985f3ee4dc103d01 |
| Base APK SHA-256 | 02d488c5fa23fa49151438a613cc2efc66345bb7043325d55f928a2720aae699 |
| Bundle | Base APK 11.7 MB, arm64-v8a split 4.8 MB, xhdpi split 2.6 MB, 19.2 MB combined |
| minSdk / targetSdk | 26 / 35 (compileSdk 35) |
| Code base | Kotlin and Java, Gradle build, single classes.dex of 8.2 MB, native libraries |
| Source of the package | APKPure mirror. Package name, developer and version were checked against the live Google Play listing on 22 August 2026 before the download, and the hash of the file matches the hash published by the mirror for this version |
| Data Protection Officer | Not found in the listing or in the binary strings. UNVERIFIED |

Supervisory competence: the publisher of record is established in Eindhoven. The Datenschutzbehörde is the natural first contact for an Austrian-initiated matter, and the Dutch Autoriteit Persoonsgegevens could be the lead authority if Össur Europe B.V. is the main establishment in the EU. The question is raised and not settled here.

## Architecture & Data Flow

The analysis used apktool without sources on the base APK for the manifest and resources, and unzip with strings and targeted searches over classes.dex for class and method names, endpoints and secret patterns. No decompiler and no full smali dump was used. Findings rest on string and class name evidence.

| Layer | Observed | Source |
|---|---|---|
| Device link | BRSP Bluetooth serial bridge with the Artix command protocol, authorisation classes, firmware update classes | classes.dex, package bluetooth |
| Cloud channel | AWS Mobile SDK with SQS, SimpleDB, S3 clients injected through Hilt, AwsRepository and AWSCommand classes | classes.dex, packages app.data.repo.aws and bluetooth_bridge |
| Licensing | Endpoint https://license.touchbionics.com/ | classes.dex |
| Local data | RecordingDatabase and AllCountsDatabase class names, stated by the vendor to be non-functional | classes.dex, vendor reply |
| Backup | allowBackup true with empty rule files | AndroidManifest.xml, res/xml |
| Scanning | QR and barcode scanning with bundled on-device ML Kit models | assets |

## Findings

### C1: A real AWS account ID and SQS queue URL are hardcoded in the shipped app, next to repository classes for hand-specific commands and records

**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 CRITICAL on 23 August 2026, reassessed in this report**

The app bundles the AWS Mobile SDK (SQS, SimpleDB, S3 and credential-provider classes) and contains in plaintext the queue URL https://sqs.us-east-1.amazonaws.com/874662143550/MyGrips-Shared, which names the real AWS account ID 874662143550. The queue name matches the app's grip-sharing feature. Beside it sit an AwsSimpleDbRepository class with methods named getCommandsForHand and updateRecordForHand and a class AWSCommandPacket inside the app's own bluetooth package. The identifiers are public in every copy of the app. An identifier alone does not grant access. The vendor stated that grip submissions are reviewed by staff before any grip is made available to other users, that the identifiers do not by themselves grant access, and that additional access restrictions were applied to the channel after this notice. RFI-IRFOS did not read from, write to or inspect the access policy of the queue, so the access policy is outside this report. The score reflects the exposure of cloud resource identifiers and not a demonstrated access.

```
https://sqs.us-east-1.amazonaws.com/874662143550/MyGrips-Shared
https://s3-us-west-1.amazonaws.com
https://license.touchbionics.com/
```

```
Lcom/touchbionics/myilimb/app/data/repo/aws/AwsSimpleDbRepository$getCommandsForHand$2
    ;
Lcom/touchbionics/myilimb/app/data/repo/aws/
    AwsSimpleDbRepository$updateRecordForHand$2;
Lcom/touchbionics/myilimb/app/data/repo/aws/AwsSimpleDbRepository;
Lcom/touchbionics/myilimb/app/data/repo/aws/AwsThings;
Lcom/touchbionics/myilimb/app/di/AwsModule_ProvideAwsRepositoryFactory;
Lcom/touchbionics/myilimb/app/di/AwsModule_ProvideAwsS3ClientFactory;
Lcom/touchbionics/myilimb/app/di/AwsModule_ProvideAwsSimpleDbClientFactory;
Lcom/touchbionics/myilimb/app/di/AwsModule_ProvideAwsSqsClientFactory;
Lcom/touchbionics/myilimb/app/di/AwsModule_ProvideCredentialsFactory;
Lcom/touchbionics/myilimb/bluetooth/AWSCommandPacket;
Lcom/touchbionics/myilimb/bluetooth_bridge/repo/AWSCommand;
Lcom/touchbionics/myilimb/bluetooth_bridge/repo/AwsRepository;
```

The queue name corresponds to the app's own strings custom_grip_share (Share my grip) and custom_grip_scan_qr (Scan QR to import my grip), confirmed in res/values/strings.xml. The Hilt module classes show that SQS, SimpleDB and S3 clients are wired into the app. The class names show that the engineers modelled AWS as a transport for hand-associated records and commands. No AKIA-format static key and no Cognito identity pool ID literal was found in the string pool, so the credential mechanism was not identified.

Not tested: whether the queue accepts requests from unauthenticated parties, the pay-

load shape and trigger conditions of getCommandsForHand and updateRecordForHand, and whether anything arriving through this channel can reach the actuators of a prosthesis or is limited to grip configuration data. The AWS SDK credential helper AWSKeyValueStore caches credentials with Android Keystore backed AES-GCM, which protects cached credentials on the device and says nothing about the server side policy of the queue.

Vendor statement of 17 September 2026, recorded as the vendor's answer and not verified from the binary: the queue supports the grip-sharing feature, staff review every submission before publication, no submission is published automatically, the account ID and queue URL do not by themselves grant access, and after this notice the configuration was reviewed, additional access restrictions were applied, and further improvements are under evaluation. The vendor gave no release window for them.

**Impact:** The people affected are wearers of i-Limb and i-Digits prostheses who share or import grip presets. A grip preset is calibrated to one person's residual-limb muscle signals, so it is adjacent to health data about that person. The vendor's statement that submissions are reviewed by staff and that access was restricted addresses the main concern. This report did not verify what metadata travels with a shared grip.

**Fix:** Keep the queue policy restricted to authenticated app principals, remove cloud resource identifiers from the shipped binary where the design allows, and document the authorisation model of the grip-sharing channel.

### H1: Legacy engineering, test and CAN-bus command classes ship in the patient-facing app, behind a device-level authorisation concept

**LOW, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B), editorial severity MEDIUM, disclosed as HIGH on 23 August 2026, re-assessed in this report**

The patient-facing app contains a complete legacy Bluetooth serial-bridge layer called BRSP with a proprietary command protocol called Artix. The class inventory includes ArtixBtCanCommands (a CAN-bus-level command relay towards the finger-motor controllers of a hand), the command dictionary iLimbs_CommsDictionary, firmware update classes, the constant CMD_BLE_BRSP_ENABLE_UNIT_TESTS and a SampleApp class. The binary also shows an authorisation concept. The vendor stated that the CAN-related class belongs to unreleased devices and is not active in the distributed app, that the test-related code consists of stubs and limited connection tests whose removal is planned, and that the authorisation check runs in the firmware of the prosthesis when a connection is established and gates the command interface as a whole. These statements are the vendor's answer and were not verified from the binary. The score reflects residual stub code in a build that talks to a device that is only reachable within Bluetooth range, which is the LOW band. RFI-IRFOS blast-radius escalation: raised from LOW/2.3 to MEDIUM because the class inventory is confirmed in the shipped build, the app controls a myoelectric hand worn by a patient, and the firmware check on which the lower rating rests is the vendor's statement and was not verified from the binary.

```
Lcom/touchbionics/myilimb/bluetooth/ArtixBtAuthorization;
Lcom/touchbionics/myilimb/bluetooth/ArtixBtCanCommands;
Lcom/touchbionics/myilimb/bluetooth/ArtixBtCanCommands_ProcessCommandResponseAdditions
    ;
Lcom/touchbionics/myilimb/bluetooth/ArtixBtGlobalConfig;
Lcom/touchbionics/myilimb/bluetooth/iLimbs_CommsDictionary;
Lcom/touchbionics/myilimb/bluetooth/iLimbsHandParameter;
Lcom/touchbionics/myilimb/bluetooth/iLimbsSystemEvent;
Lcom/touchbionics/myilimb/bluetooth/SampleApp;
Lcom/touchbionics/myilimb/bluetooth/UnitTest;
Lcom/touchbionics/myilimb/bluetooth/UnitTests;
Lcom/touchbionics/myilimb/bluetooth/DeviceUpdate;
Lcom/touchbionics/myilimb/bluetooth/DeviceUpdateCmd;
Lcom/touchbionics/myilimb/bluetooth/DeviceUpdateDoc;
Lcom/touchbionics/myilimb/bluetooth/FirmwareFileHelper;
Lcom/touchbionics/myilimb/bluetooth/FirmwareHeader;
```

```
CMD_BLE_BRSP_ENABLE_UNIT_TESTS
CMD_BLE_CONNECT_BRSP
CMD_BLE_CONNECT_BRSP_MAC
CMD_BLE_START_ARTIX_COMMS
BtCmdAuthorization, needAuth: YES
Current BRSP Security Level set to:
Can't locate the BRSP service.
```

Authorisation evidence in the binary: the classes ArtixBtAuthorization and BtCmdAuthoriza-

tion, the literal needAuth: YES, a DecodeAuthorizationMessage and InvalidAuthorizationMessageException pair, a configurable BRSP Security Level and a user-facing My security code screen (prefs_about_security). This is a stronger design than a bare client-side flag, and the vendor's statement places the enforcement point in the firmware.

The in-app copyright string spans 2013 to 2025 and the package namespace is com.touchbionics.myilimb, which is consistent with a codebase carried forward from Touch Bionics. Candidate BLE UUIDs found near the BRSP and Artix classes in the string pool are listed under Indicators. They were not confirmed against a public i-Limb specification.

Not tested: the cryptographic strength of the security code mechanism, whether the shipped interface reaches the test and CAN-bus classes, and whether the firmware check covers every command. No device was paired and no command was sent.

**Impact:** The people affected are wearers of the i-Limb Quantum, i-Limb Ultra, i-Limb Access, i-Digits Quantum and i-Digits Access prostheses. The firmware level check that the vendor describes is the control that protects them. The remaining point is that test and engineering code travels in every installed copy.

**Fix:** Remove the test stubs, the SampleApp class and the engineering command classes from the patient build, and document in writing which commands the firmware authorisation covers.

### H2: allowBackup is true and both backup rule files are empty, so no exclusion is configured for the app's data

**LOW, CVSS v4.0 AV:P/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 1.0 (CVSS-B), disclosed as HIGH on 23 August 2026, reassessed in this report**

android:allowBackup is true and both backup configuration files exist and contain no exclusion elements, so the app's sandbox is eligible for Android's automatic backup to the user's Google account. The vendor confirmed that no backup exclusion rules are defined and that the restriction is under engineering review. The notice named a muscle-signal recording database (RecordingDatabase) and a usage-counter database (AllCountsDatabase) as the sensitive content. The vendor stated that both classes are non-functional in the Android app, that they were carried over from an earlier design and contain no operative code, and that the Android app does not record EMG data. This report accepts that statement and no longer rates the finding on muscle-signal data. What remains eligible for backup is whatever the app stores locally, which includes the data behind the About screen (hand serial number, firmware version and the security code) and session state. What exactly is stored in each file was not examined.

```
<application android:allowBackup="true" ... android:dataExtractionRules="@xml/
    data_extraction_rules"
     android:fullBackupContent="@xml/backup_rules" ...>
```

```
<!-- data_extraction_rules.xml -->
<data-extraction-rules>
    <cloud-backup />
</data-extraction-rules>

<!-- backup_rules.xml -->
<full-backup-content />
```

An empty cloud-backup element and an empty full-backup-content element place no restriction on what the platform includes. The app shows awareness of sensitive local data through a PIN-lock screen for the app itself. No exclusion was applied to the platform backup surface.

Whether the security code is stored in a form that enters the backup set was not examined, and a backup restore needs the user's own Google account.

**Impact:** The people affected are users of the app, adult wearers of a myoelectric prosthesis. A backup that includes a device serial number and a personal security code stays under the control of their own Google account.

**Fix:** Define exclusion rules in data_extraction_rules.xml and backup_rules.xml for the security code, device identifiers, session state and any database, or set allowBackup to false.

### M1: No network security configuration and no certificate pinning

**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)**

The manifest has no android:networkSecurityConfig attribute and res/xml has no network_security_config.xml. No cleartext override is declared. With targetSdkVersion 35 the platform default denies cleartext traffic, which mitigates the point. No certificate pinning exists for the account, AWS and licensing traffic (license.touchbionics.com and the AWS SQS, SimpleDB and S3 endpoints named under C1).

The vendor reply of 17 September 2026 did not address this finding.

**Impact:** Users who sign in and share grips rely on the system trust store alone.

**Fix:** Add a network security configuration with certificate pinning for the licensing host and the AWS endpoints.

## Impact Analysis

The people affected are adult wearers of myoelectric hands and fingers from Össur and Touch Bionics who use My i-Limb to configure and monitor the device. The store rates the app for all ages.

The notice raised three concerns. The first was a cloud channel with named identifiers next to classes that model hand-specific commands. The vendor answered with staff review, restricted access and the point that identifiers alone grant nothing. The second was an engineering and test command surface in the patient build. The vendor answered with an inactive CAN class, stub test code and firmware enforced authorisation. The third was backup of muscle-signal data. The vendor answered that the named databases do nothing in the Android app.

What remains is a short list. The backup rules are empty and confirmed. The stub test code and the engineering classes remain in the distributed build until a release removes them. The vendor gives no release window, so the improvements can be confirmed only by comparing shipped builds. No harm to any user is claimed by this report.

## The Complete Chain

| Step | Evidence |
|---|---|
| The app identifies a real AWS account and an SQS queue for grip sharing | queue URL string, custom_grip_share and custom_grip_scan_qr strings |
| The app contains repository classes for hand-specific commands and records | AwsSimpleDbRepository, AWSCommandPacket, AWSCommand |
| What the queue accepts and from whom | Not tested. Vendor states staff review and restricted access |
| Whether anything on this channel reaches the actuators of a prosthesis | UNVERIFIED. Vendor states grip submissions are reviewed and that firmware authorisation gates the command interface |
| Whether a newer build contains the stated improvements | Not checked in this report, the audited build is 1.0.16 |

The chain ends at open questions that the vendor has answered in writing. The access policy of the queue and the firmware enforcement point cannot be verified from the app package.

## Inference Data and Control Data

The real-time muscle-signal graph of the app (GraphSignalData, GraphThresholdData, menu entry myo-graph) displays a user's residual-limb muscle activity on screen. Muscle activity tied to an amputation plausibly falls within data concerning health under Article 9(1) GDPR. The vendor stated that the Android app does not record EMG data, so this report does not rate stored recordings.

The control capabilities in the binary are the firmware update classes (DeviceUpdate, DeviceUpdateCmd, DeviceUpdateDoc, FirmwareFileHelper, FirmwareHeader) and the AWS repository methods named above. They confirm that the app can push firmware or configuration to a hand. Their exercise was not observed.

Bystander data: a grip preset calibrated to one wearer can be shared and imported by another, so the shared preset is adjacent to health data about its creator. What metadata travels with a shared grip was not verified. Non-events, a household graph and notification mirroring do not apply, because no notification listener and no location based co-location logic exists in the manifest.

## Observation: PEGI 3 Rating on a Medical App

This is an observation without a severity. The live Play listing, checked on 22 August 2026, shows the category Medical and the content rating PEGI 3 (Everyone), the lowest available rating. The app configures and monitors a myoelectric prosthetic hand and shows a real-time muscle-signal graph. Its actual users are adult amputee patients. The app has no age gate, and a PEGI 3 rating does not imply one, so this is a rating-transparency note and not a missing safeguard.

## Data Protection: Article by Article

| Article | Relevance | Finding |
|---|---|---|
| 5(1)(c) | Data minimisation, no exclusion applied to the backup surface | H2 |
| 9(1) | Muscle activity of an amputee shown in the app, context only | Inference data |
| 25, 25(2) | Protection by design and by default for the cloud channel, command surface and backup | C1, H1, H2 |
| 32(1)(a), (b) | Integrity and confidentiality of the channel, the command link and the backup | C1, H1, H2, M1 |
| 32(1)(d) | Regular testing of security measures for a cloud resource named in the binary | C1 |

## Regulatory & Legal Landscape

The bases are Regulation (EU) 2016/679 (GDPR) with Articles 5, 9, 25 and 32. The disclosure follows ISO/IEC 29147 and rests on the freedom of research under Article 17 of the Austrian Staatsgrundgesetz.

The Datenschutzbehörde (dsb@dsb.gv.at) and the European Data Protection Supervisor (edps@edps.europa.eu) were in copy of the first notice.

## Indicators of Compromise & Reproducible Evidence

Every item can be reproduced from the named package. No Össur server or AWS resource was contacted and no device was paired.

| | |
|---|---|
| Package | com.ossur.myilimb.app 1.0.16 (130) |
| XAPK | 7b0072f4245244a8525ed2d7ca9119537041110b14df2ae6985f3ee4dc103d01 |
| Base APK | 02d488c5fa23fa49151438a613cc2efc66345bb7043325d55f928a2720aae699 |
| SQS | https://sqs.us-east-1.amazonaws.com/874662143550/MyGrips-Shared |
| AWS acct | 874662143550 |
| S3 | https://s3-us-west-1.amazonaws.com |
| Licence | https://license.touchbionics.com/ |
| Class | com.touchbionics.myilimb.bluetooth.ArtixBtCanCommands |
| Constant | CMD_BLE_BRSP_ENABLE_UNIT_TESTS |
| Log | BtCmdAuthorization, needAuth: YES |
| Manifest | android:allowBackup=true, empty data_extraction_rules.xml and backup_rules.xml |
| Contacts | playstore_agent@ossur.com, thbaldursson@emblamedical.com |
| Policy | https://www.ossur.com/global/privacy-policy |

Candidate Bluetooth UUIDs found in the string pool near the BRSP and Artix classes. They are named as candidates by contextual proximity and were not confirmed against a public i-Limb specification.

```
0A1934F5-24B8-4F13-9842-37BB167C6AFF
18CDA784-4BD3-4370-85BB-BFED91EC86AF
99564A02-DC01-4D3C-B04E-3BB1EF0571B2
A87988B9-694C-479C-900E-95DFA6C00A24
BF03260C-7205-4C25-AF43-93B1C299D159
DA2B84F1-6279-48DE-BDC0-AFBEA0226079
FDD6B4D3-046D-4330-BDEC-1FD0C90CB43B
```

## Disclosure Timeline & Outcome

| Date | Event |
|---|---|
| 23 Aug 2026 | First notice REF SSURILIMB-2026-R1 to playstore_agent@ossur.com with the Datenschutzbehörde and the EDPS in copy (sent in the night of 22 to 23 August 2026 UTC and dated 23 August in the notice). Three questions asked. Publication stated as 21 November 2026. |
| 12 Sep 2026 | Follow-up with the three questions repeated, answer requested by 19 Sep 2026. No reply had reached RFI-IRFOS by then. |
| 13 Sep 2026 | According to the vendor, the report reached its security organisation on this date. |
| 17 Sep 2026 | Written reply of the Embla Medical security officer answering the three questions, with changes to the intake routing and access restrictions on the AWS channel. |
| 18 Sep 2026 | RFI-IRFOS acknowledges the reply and asks three timeline questions. The vendor answers the same day that target versions and release windows are not communicated externally. |
| 17 Oct 2026 | Further mail asking for the shipped version of each of the three items. No reply. |
| 15 Nov 2026 | Mail 6 days before publication, 84 days after the notice and 29 days after the mail of 17 October. It repeats the three open items with an answer date of 20 November 2026, sets out the reassessed severities and corrects the publication date: 21 November 2026 is right and 20 November 2026 in the mails of 18 September and 17 October was wrong. No reply. |
| 21 Nov 2026 | Publication date as stated in the first notice and in the mail of 15 November 2026. No reply to the mails of 17 October and 15 November, 35 days and 6 days after they were sent. |

Outcome as of 21 November 2026: a substantive written reply was received on 17 September 2026 and a short answer on 18 September 2026. The three open items wait for shipped builds. No reply to the mails of 17 October and 15 November 2026.

## What Össur Got Right

The binary shows a real device-level authorisation concept, with ArtixBtAuthorization, BtCmdAuthorization, a configurable BRSP Security Level and a user-visible security code screen, and the vendor places its enforcement in the firmware. AWS credentials cached by the SDK are encrypted at rest with Android Keystore backed AES-GCM. No advertising, analytics, session-replay or China or sanctioned-jurisdiction SDK is present in the dependency set, which agrees with the Play Data Safety statement that no data is shared with third parties. QR and barcode scanning runs on the device with bundled ML Kit models and no cloud vision call. The privacy notice and the terms ship offline in ten languages inside the app. targetSdkVersion 35 denies cleartext traffic by default, and no hardcoded Firebase or Google API key and no AKIA or sk_ shaped secret was found.

The vendor answered within days of the report reaching its security organisation, corrected the intake routing for the Play Store contact address, applied access restrictions to the AWS channel as a direct result of the notice, and gave technically specific answers to all three questions.

## Residual Risk & Recommendations

| Priority | Action | Finding |
|---|---|---|
| 1 | Add exclusion rules or set allowBackup to false | H2 |
| 2 | Remove test stubs, SampleApp and unreleased device classes from the patient build | H1 |
| 3 | Complete the AWS channel improvements and remove cloud resource identifiers from the binary where possible | C1 |
| 4 | Add a network security configuration with certificate pinning | M1 |

Residual risk: every installed copy of version 1.0.16 contains the items above until a release removes them. This report describes version 1.0.16 only. The weekly comparison of shipped builds promised in the notice has no recorded result in the case folder, so the vendor’s stated improvements are not confirmed in a shipped build.

**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 plus the live Google Play listing. No Össur servers or AWS resources were probed and no device was paired. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Arts. 5, 9, 25, 32. RFI-IRFOS ZVR 1015608684, GISA 39261441. REF SSURILIMB-2026-R1.