# Security & Privacy Disclosure, Final Report

## Ottobock Cockpit for Android (com.ottobock.prosthetics.ll.cockpit)

A storage account key in the public package, a device name that carries type and serial number, and file commands for a prosthesis, all in an app with more than 100,000 installations.

**PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED 20 NOVEMBER 2026. NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026.**

| | |
|---|---|
| **Target** | Otto Bock Healthcare Products GmbH, Vienna (group: Ottobock SE & Co. KGaA) |
| **Versions Audited** | 2.9.1.5 / 20901005 (analysis 2026-08-22) |
| **Notice / Publication** | 2026-08-22 / 2026-11-20 (90 days, unchanged) |
| **Findings** | 8: 1 Critical, 1 High, 3 Medium, 3 Low (H1 and H2 reassessed from High) |
| **Status** | NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026 |
| **SHA-256 (base APK)** | `17e203c1b57dac6a47098a9f2fe24cafbf72fe036ec51ffac6df5650fe7a09b2` |

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 6

5 Findings 7
- 5.1 C1: Account-level Azure Storage key for sampktsproduction in plaintext in the distributed package . . . 7
- 5.2 H1: Two backend generations remain addressed by the shipped app, most hostnames still resolve . . . 8
- 5.3 H2: Prosthesis type and serial number are part of the Bluetooth device name the app parses . . . 9
- 5.4 H3: File write, append and erase commands for the device's onboard storage, integrity checksum is CRC64 . . . 10
- 5.5 M1: No certificate pinning and no network security configuration for any backend host . . . 11
- 5.6 M2: Consent withdrawal is offered only by email although a consent API exists 11
- 5.7 M3: The privacy policy link referenced in the app returns 404 . . . 12
- 5.8 M4: End-of-life UI framework and maintenance-only release cadence . . . 12

6 Impact Analysis 13

7 The Complete Chain 13

8 Medical Device Context: MDR (EU) 2017/745 Annex I Section 17.2 14

9 Data Protection: Article by Article 15

10 Regulatory & Legal Landscape 16

11 Indicators of Compromise & Reproducible Evidence 16

12 Disclosure Timeline & Outcome 17

13 What Ottobock Got Right 17

14 Residual Risk & Recommendations 18

## Executive Summary

Ottobock Cockpit is the companion app for Ottobock's electronic prosthetic knees and orthoses, published by Otto Bock Healthcare Products GmbH in Vienna with more than 100,000 installations on Google Play. On 22 August 2026 RFI-IRFOS sent eight findings from a root level code analysis of version 2.9.1.5 under REF OTTOBOCKCOCKPIT-2026-R1.

The most serious finding is an Azure Storage connection string with an account key in plaintext inside the assembly Cockpit.Api.dll. The account sampktsproduction resolves in public DNS. The key is account-wide, so a valid key would reach every container of the account and not only the path the app reads. The validity of the key was not tested.

Two further findings concern the prosthesis itself. The app parses a device name that carries the product type and the serial number, and the app holds file write, append and erase commands for the onboard storage of the device with a CRC64 checksum as the only integrity mechanism found in the extracted assemblies. Neither was exercised against a device. Four lower findings cover live legacy hosts, missing certificate pinning, consent withdrawal by email only and a dead privacy link.

Two of the severities sent in the first notice are lowered in this report, because the evidence supports a lower band than the notice stated. Ottobock sent no substantive reply to the first notice or to the two follow-ups of 12 September and 17 October 2026 or to the final notice of 15 November 2026.

**Scope:** Root level code analysis of the Google Play release 2.9.1.5 (versionCode 20901005): manifest, resources and the 123 .NET assemblies at string level, plus passive public DNS and single unauthenticated HEAD requests. No Ottobock server or account was authenticated against, the storage key was not used, and no device was contacted. Dynamic analysis is not part of this report.

| ID | Severity | Title |
|---|---|---|
| C1 | CRITICAL | Account-level Azure Storage key for sampktsproduction in plaintext in the distributed package |
| H1 | LOW | Two backend generations remain addressed by the shipped app, most hostnames still resolve |
| H2 | MEDIUM | Prosthesis type and serial number are part of the Bluetooth device name the app parses |
| H3 | HIGH | File write, append and erase commands for the device's onboard storage, integrity checksum is CRC64 |
| M1 | MEDIUM | No certificate pinning and no network security configuration for any backend host |
| M2 | MEDIUM | Consent withdrawal is offered only by email although a consent API exists |
| M3 | LOW | The privacy policy link referenced in the app returns 404 |
| M4 | LOW | End-of-life UI framework and maintenance-only release cadence |

### Finding Status at a Glance

The table shows the severity sent in the first notice of 22 August 2026 next to the severity in this report. Two findings were reassessed after the evidence was re-read. The other severities stand.

| ID | Sent 22 Aug 2026 | This report | Basis |
|---|---|---|---|
| C1 | CRITICAL | CRITICAL | CVSS 9.1. Key validity not tested. |
| H1 | HIGH | LOW | Inventory of live hosts, no weakness shown. CVSS 0.0. |
| H2 | HIGH | MEDIUM | Name pattern shown, advertising before pairing inferred and not captured. CVSS 5.3. |
| H3 | HIGH | HIGH | CVSS 6.0, raised to HIGH for a load-bearing prosthesis, reason stated in the finding. |
| M1 | MEDIUM | MEDIUM | CVSS 6.3. |
| M2 | MEDIUM | MEDIUM | Editorial, reason stated in the finding. |
| M3 | MEDIUM/LOW | LOW | Dead link, CVSS 0.0. The dual label of the notice is settled at LOW. |
| M4 | LOW | LOW | Context only. |

## Subject & Operator Analysis

Ottobock Cockpit is the companion app for adjusting Ottobock's electronic prosthetic knees and orthoses, among them C-Leg, Genium, GeniumX3 and GeniumX4. The manufacturer of record named in the app is Otto Bock Healthcare Products GmbH, Brehmstraße 16, 1110 Wien, Austria, telephone +43 1 523 37 86. The parent group is Ottobock SE & Co. KGaA, Duderstadt, Germany. Google Play shows more than 100,000 installations and a PEGI 3 rating. The store listing states that the product meets the applicable European requirements for medical devices.

| Item | Value |
|---|---|
| Package | com.ottobock.prosthetics.ll.cockpit |
| Version | 2.9.1.5 (versionCode 20901005) |
| File size | 42,287,736 bytes |
| SHA-256 | 17e203c1b57dac6a47098a9f2fe24cafbf72fe036ec51ffac6df5650fe7a09b2 |
| Signing certificate fingerprint | 1ded03cf7a2df894cfcfb945627d77230a653ca8 (partial, taken from a mirror listing) |
| minSdk / targetSdk | 26 (Android 8.0) / 34 (Android 14) |
| Code base | Xamarin.Forms on .NET, 123 assemblies in assemblies/ assemblies.blob, SQLite through SQLCipher |
| Privacy and support contacts in the app | cockpit@ottobock.com, myottobock@ottobock.com, info.austria@ottobock.com |
| Data protection officer | not found in the binary or in the reachable documentation (UNVERIFIED) |

The successor app connectgo. by ottobock. (com.ottobock.connectgo) has 500 plus installations according to the store, against 100,000 plus for Cockpit. On the store's bracketed counts Cockpit is about 200 times larger, so the older app carries the larger share of users. Store text for Cockpit says the app may share app information and performance data with third parties, and the store text for connectgo says no data is shared with third parties.

Supervisory competence: the manufacturer's registered address for this product is in Vienna, which supports Austrian competence of the Datenschutzbehörde. If Ottobock SE & Co. KGaA in Duderstadt is the main establishment for this processing, a German authority would be competent. The question is raised and not settled here.

## Architecture & Data Flow

Cockpit is a Xamarin application. The Java layer holds only the Mono bootstrap. The application logic sits in 123 .NET assemblies inside a custom assembly store, which RFI-IRFOS unpacked and read at string level.

| Layer | Observed | Source |
|---|---|---|
| Bluetooth to the prosthesis | Basic, Vienna and Unified Ottobock protocol stacks. Library DeviceRemoting.dll states in a doc comment that it provides virtual device communication to be consumed by Ottobock apps. Commands include file transfer (Commanding.MPK.dll) and a password request. | DeviceRemoting.dll, Commanding.MPK.dll, OBHC.CAA.ViennaRemoting.UNE.dll |
| Backend | Newer REST hosts under swservice.ottobock.com for access, auth, consents, device, patients, profile and trial. Older WCF service at mobileservice.ottobock.com. Environment selector at ob-environment.azurewebsites.net. | Cockpit.Api.dll |
| Storage | Azure Blob account sampktsproduction, path files/cockpit/{0}/ for the device compatibility list. | Cockpit.Api.dll |
| Consent | Server-synchronised client with accept, my and terms endpoints. | OBApiClients.ConsentService.dll |
| Local storage | SQLite encrypted with SQLCipher. | libsqlcipher.so, SQLitePCLRaw.*.sqlcipher |
| Telemetry | Microsoft App Center Analytics and Crashes only. No advertising or attribution SDK in any of the 123 assemblies. | assembly inventory |

The shared device library matters beyond Cockpit. Its own doc comment says it serves Ottobock apps in the plural, so a weakness in the shared command layer would not stay inside one app.

## Findings

### C1: Account-level Azure Storage key for sampktsproduction in plaintext in the distributed package

**CRITICAL, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 9.1 (CVSS-B)**

The assembly Cockpit.Api.dll carries a complete Azure Storage connection string including an account key. The key belongs to the shared-key model, so it covers every container, blob, table and queue of the account sampktsproduction and not only the path files/cockpit/ that the app reads. The attack precondition (AT:P) is that the key has not been rotated. RFI-IRFOS did not authenticate with the key and did not test its validity.

```
CloudStorageConnectionString
DefaultEndpointsProtocol=https;AccountName=sampktsproduction;AccountKey=
    ekBOQwWDR6qEGf70tb9nvScZxGIQ7SkKqi8s2qVbl4GHSxfYK1kbiDKS/0MQA3049S8ZXB9y2VMt+AStho
    +ofQ==;EndpointSuffix=core.windows.net

DeviceCompatibilityListBaseUrlTemplate
https://sampktsproduction.blob.core.windows.net/files/cockpit/{0}/
```

```
$ getent hosts sampktsproduction.blob.core.windows.net
57.150.91.65
$ curl -sk -o /dev/null -w "%{http_code}" https://sampktsproduction.blob.core.windows.
    net/files/cockpit/
404
```

The 404 shows that the host answers and that anonymous container listing is not enabled. It says nothing about the key. The storage account name contains the word production. The URL template shows that the app downloads a device compatibility list from files/cockpit/. A holder of a valid account key could replace such content, and could reach any other container in the account. What else the account stores was not analysed.

A key inside a public package cannot be recalled from the installed copies. Each copy of version 2.9.1.5 carries it. The only effective remedy is rotation of the key on the account side.

**Impact:** Every copy of Cockpit 2.9.1.5 on the Play Store carries this key. If the key is valid, any person who unpacks the app can read, overwrite or delete the account's content. The app is the companion for electronic prosthetic knees and orthoses, so the people downstream of this account are prosthesis users and their prosthetists, and the content they rely on includes the device compatibility list the app downloads from this account.

**Fix:** Rotate the account key now, whether or not it is still valid. Remove account keys from client binaries and serve client content through read-only, time-limited and container-scoped access. Review the storage account's logs for access that did not come from known app traffic and enable per-request logging if it is off.

### H1: Two backend generations remain addressed by the shipped app, most hostnames still resolve

**LOW, 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, reassessed in this report**

The binary addresses 11 endpoint URLs on 10 distinct hostnames across an older WCF service and a newer REST family. Eight hostnames resolve in public DNS on 22 August 2026. Two do not. The inventory shows live legacy surface in a still-distributed app. No weakness of any of these hosts was tested or demonstrated, so CVSS scores the finding at 0.0.

```
https://access.swservice.ottobock.com
https://auth.swservice.ottobock.com
https://consents.swservice.ottobock.com
https://device.swservice.ottobock.com
https://patients.swservice.ottobock.com/
https://profile.swservice.ottobock.com
https://trial.swservice.ottobock.com/
https://mobileservice.ottobock.com/CockpitService.svc/json
https://mobileservice.ottobock.com/CockpitService.svc/json/RegisterNewDevice
https://ob-environment.azurewebsites.net/api/
https://my.ottobock.com/info
```

| Host | DNS on 22 Aug 2026 | Unauthenticated HEAD |
|---|---|---|
| access.swservice.ottobock.com | resolves (Azure) | not recorded |
| auth.swservice.ottobock.com | resolves (Azure) | 200 |
| consents.swservice.ottobock.com | resolves (Azure) | 200 |
| device.swservice.ottobock.com | resolves (Azure) | not recorded |
| patients.swservice.ottobock.com | resolves (Azure) | not recorded |
| profile.swservice.ottobock.com | resolves (Azure) | not recorded |
| mobileservice.ottobock.com | resolves (Azure) | 404 on the service path |
| my.ottobock.com | resolves (Azure) | not recorded |
| trial.swservice.ottobock.com | NXDOMAIN | none |
| ob-environment.azurewebsites.net | NXDOMAIN | none |

The host ob-environment.azurewebsites.net with a resource named AvailableEnvironments follows the pattern of a remote environment selector. It does not resolve today. Whether the successor app connectgo carries a comparable selector was not determined here (UNVERIFIED).

**Impact:** The same prosthesis users who run Cockpit depend on a backend that the operator appears to be retiring in parts while the app still addresses all of it. The finding supports the point that an app installed on more than 100,000 devices is not a legacy app in practice. It does not show that any host is weak.

**Fix:** Publish a decommissioning plan for the legacy WCF service and the trial and environment hosts. Remove hostnames from the app that are no longer meant to be reached. Keep an inventory that matches the hostnames in shipped builds.

### H2: Prosthesis type and serial number are part of the Bluetooth device name the app parses

---

**MEDIUM, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.3 (CVSS-B), disclosed as HIGH on 22 August 2026, reassessed in this report**

The assembly OBHC.CAA.ViennaRemoting.UNE.dll contains a regular expression that parses a device name of the form OB_<Type>[<BtVersion>]_SN<Serial>. The expression shows that the component's name carries type and serial number. RFI-IRFOS did not capture Bluetooth traffic. That the name is visible to an unpaired scanner is an inference from the app's discovery logic and is not a measured fact, so the finding is rated at the CVSS band of its demonstrated part.

```
OB_(?<Type>.*?)(\[(?<BtVersion>[0-9])\])*_SN(?<Serial>[0-9]*)
```

The pattern is the app's own parser for the device name. A name that includes the product type and the exact serial number is a persistent identifier. If the component transmits this name while unpaired, a person with a generic Bluetooth scanner in range could learn that someone nearby wears a prosthesis of a given model and could recognise the same serial again on a later encounter. The first notice described this as proven. This report states it as the consequence that follows if the name is advertised before pairing, and marks the advertising behaviour itself as UNVERIFIED because no capture was made.

Whether a type and serial number alone amount to health data about an identifiable person under Article 9 GDPR depends on whether an observer can link them to a person. That is a question for the controller and the supervisory authority, which is why the question in the first notice asked whether a data protection impact assessment exists.

**Impact:** The people affected are wearers of Ottobock electronic prostheses and orthoses, many of them adults with an acquired amputation or older adults. If the device name is advertised as the parser suggests, they could be recognised by a bystander without any action on their part. The realistic harm is unwanted disclosure of a disability and tracking of one device across places, not access to the device.

**Fix:** Use a rotating, non-identifying advertising identifier and move type and serial number into the authenticated session. Document the decision in a data protection impact assessment under Article 35 GDPR.

### H3: File write, append and erase commands for the device's onboard storage, integrity checksum is CRC64

**MEDIUM, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N, 6.0 (CVSS-B), editorial severity HIGH**

The Bluetooth command layer (Commanding.MPK.dll) includes primitives that write, append and erase files on the prosthesis's own remote storage. The only integrity mechanism found for this channel in the extracted assemblies is CaaChecksum.dll, a CRC64 implementation. A command named RequestPasswordDeviceCommand shows that some password step exists before commands are accepted. Its derivation and its enforcement for the file commands were not determined. Nothing was sent to a real device. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.0 to HIGH because a write path aimed at the storage of a load-bearing prosthesis puts the physical safety of its wearer behind the integrity question, a consequence the technical scope of CVSS does not capture.

```
Commanding.MPK.dll
ReadX4FileMetaDataAsync
WriteX4FileContentAsync
Store File on Remote Host command failed
Append Data to Remote File command failed
Erase Remote File Info command failed
Retrieve File Info command failed

CaaChecksum.dll
CRC64 does not feature precalculated tables, because the lookup index is integer based
    ...

OBHC.CAA.ViennaRemoting.UNE.dll
RequestPasswordDeviceCommand
```

This is a capability finding. The evidence is the presence of the commands and the absence of any cryptographic integrity or signing string around them. It is not an exploit. Dynamic analysis against hardware is outside the scope of this report. No .NET decompiler was available, so the evidence is at string level and not at source level.

CRC64 detects transmission errors. It does not authenticate the sender and does not stop a deliberate modification. Whether the device requires the password step before it accepts a file write is the question the manufacturer can answer and an outside analyst cannot answer from the app alone.

**Impact:** The commands are aimed at a limb that a person stands and walks on. Users of the C-Leg, Genium, GeniumX3 and GeniumX4 family are adults who rely on the knee's stance and swing control. A weakness in the write path would matter to them more than a weakness in a typical consumer accessory, which is the reason for the severity set here.

**Fix:** Document which authentication and integrity controls protect the file commands on the device side. Replace non-cryptographic checks on the write path with authenticated integrity protection. Include the file-command class in the cybersecurity risk assessment under MDR Annex I Section 17.2.

### M1: No certificate pinning and no network security configuration for any backend host

**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 package contains no res/xml/network_security_config.xml and the manifest references none. No TrustManager, ServerCertificateValidationCallback or pinning string was found in crypto.dll or Cockpit.Api.dll. All backend hosts rely on the platform trust store. With minSdk 26 and targetSdk 34 cleartext is blocked by platform default, which is adequate baseline hygiene.

The channels concerned include the authentication, consent and device endpoints listed under H1. An attacker would need a position on the network path and a certificate the device trusts, which is why the attack requirements are rated as preconditions.

**Impact:** Prosthesis users who log in or register a device send account and device data over channels that depend solely on the system trust store.

**Fix:** Add a network security configuration with pinning for the authentication, consent and device hosts and a documented rotation procedure.

### M2: Consent withdrawal is offered only by email although a consent API exists

**MEDIUM, 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)**

The app ships a server-synchronised consent client (OBApiClients.ConsentService.dll with the paths /api/v1/consent/my, /api/v1/consent/accept and /api/v1/consent/terms). In every one of the 11 localised consent texts found, the only withdrawal route is an email to cockpit@ottobock.com. CVSS does not score consent design, so the rating is editorial. RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because Article 7(3) states a direct requirement on the ease of withdrawal and the affected users are patients of a medical device manufacturer, a context the CVSS technical scope does not capture.

```
/api/v1/consent/my
/api/v1/consent/accept
/api/v1/consent/terms
```

Dutch consent text as found: ”Ik ga er uitdrukkelijk mee akkoord dat de prothesecomponent... Deze toestemming kan ik door middel van een e-mail aan cockpit@ottobock.com altijd herroepen.” The English meaning is that the user may always revoke this consent by email to cockpit@ottobock.com.

**Impact:** Prosthesis users give consent inside the app in one step and must leave the app and write an email to withdraw it. Article 7(3) requires that withdrawal is as easy as giving consent.

**Fix:** Add an in-app withdrawal control that calls the existing consent API, and keep the email address as an additional route.

### M3: The privacy policy link referenced in the app returns 404

**LOW, 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)**

The string table of Cockpit.dll references a data_privacy.pdf on ottobock.com. On 22 August 2026 the link redirected with 307 to a localised path and then returned 404. The neighbouring compatible.pdf link in the same string table resolves. CVSS does not score this transparency gap.

```
https://www.ottobock.com/media/local-media/sonstiges/cockpit-app/data_privacy.pdf
$ curl -sIL https://www.ottobock.com/media/local-media/sonstiges/cockpit-app/
    data_privacy.pdf
HTTP/2 307  location: /de-de/media/local-media/sonstiges/cockpit-app/data_privacy.pdf
HTTP/2 404
```

**Impact:** A user who follows the link inside the app finds no privacy information at the address the app gives.

**Fix:** Restore the document at the referenced address or update the reference in the next build, and name a data protection officer in it.

### M4: End-of-life UI framework and maintenance-only release cadence

**LOW, 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)**

The UI layer is Xamarin.Forms, for which Microsoft ended official support in May 2024. The two most recent changelog entries cited in the first notice read ”Minor update to ensure Google Play store compatibility”. targetSdkVersion 34 is maintained. The finding gives context for H1 and H3 and has no direct exploit path, so CVSS scores it at 0.0.

The same build carries the Bluetooth command layer discussed under H3 and the legacy backend discussed under H1. An unsupported UI framework does not itself create a weakness. It limits the vendor’s ability to receive upstream fixes.

**Impact:** Users of the 100,000 plus installations rely on an app whose framework no longer receives upstream fixes.

**Fix:** Plan the migration to a supported framework, for example .NET MAUI, and publish the intended end-of-support date of the current app.

## Impact Analysis

The people affected are users of Ottobock's electronic prosthetic knees and orthoses and the prosthetists who adjust them with this app. Many are adults with an acquired amputation, and many are older. The app is rated PEGI 3, which describes a general audience and does not describe the real population.

C1 puts a credential for a production storage account in every copy of the app. If the key is valid, the account's content is exposed to anyone who unpacks the package, including content the app downloads and trusts. H2 concerns bystanders as well as users, because a device name that carries type and serial number could be read by anyone in range if it is advertised before pairing. H3 concerns the integrity of the channel that tells a load-bearing limb what to do.

What is demonstrated is the presence of the key, the presence of the parser pattern and the presence of the file commands. What is not demonstrated is exploitation of any of them. This report does not claim harm to a user.

## The Complete Chain

Three chains follow from the evidence. Each step names the file that supports it, and steps that rest on inference are marked.

| Chain | Step | Evidence |
|---|---|---|
| A. Account key | Anyone downloads the public Play package | APK SHA-256 17e203c1b57dac6a47098a9f2fe24cafbf72fe036ec51ffac6df5650fe7a09b2 |
| | The key sits in Cockpit.Api.dll as plaintext | string table of Cockpit.Api.dll |
| | The account host resolves and answers | DNS 57.150.91.65, HEAD 404 |
| | If the key is valid, read, write and delete across the account follow | Azure shared-key model (validity UNVERIFIED) |
| | The app trusts content from files/cockpit/ for its device compatibility list | device compatibility list URL template in Cockpit.Api.dll |
| B. Device name | The component carries type and serial in its name | regular expression in OBHC.CAA.ViennaRemoting.UNE.dll |
| | Visible to an unpaired scanner (inferred, no capture) | UNVERIFIED |
| | A persistent identifier allows recognition across encounters | follows from the serial number |
| C. Command channel | Companion app holds file write, append and erase commands | Commanding.MPK.dll |
| | Only a CRC64 checksum is found for the channel | CaaChecksum.dll |

| Chain | Step | Evidence |
|---|---|---|
| | A password command exists, its enforcement is not known | password request command in ViennaRemoting.UNE.dll |

The chains do not depend on each other. The first is a storage credential issue, the second a privacy design issue and the third an integrity question on a safety-relevant channel.

## Medical Device Context: MDR (EU) 2017/745 Annex I Section 17.2

The store listing of Cockpit states that the product meets the applicable European requirements for medical devices. Annex I Section 17.2 of Regulation (EU) 2017/745 requires software in or as a device to be developed and manufactured according to the state of the art, taking into account the principles of the development life cycle, risk management including information security, and verification and validation.

Whether the Cockpit app is itself a device or an accessory in the sense of the Regulation is for the manufacturer to state, and this report does not decide it. The question asked in the first notice is narrower: whether the file command class (H3) was part of a documented risk assessment. A written answer would show the state of the art that the manufacturer applied to the command channel.

| Article | Relevance | Finding |
|---|---|---|

## Data Protection: Article by Article

| Article | Relevance | Finding |
|---|---|---|
| 5(1)(c) | Data minimisation in an advertised device name | H2 |
| 5(1)(e) | Storage limitation, hosts that appear to be retired remain addressed | H1 |
| 5(1)(f) | Integrity and confidentiality, account key in client code | C1 |
| 7(3) | Withdrawal as easy as giving consent | M2 |
| 9 | Health-related data if the identifier is linked to a person | H2 |
| 12(1), 13 | Accessible information, privacy link returns 404 | M3 |
| 25 | Data protection by design for key handling and for the advertised name | C1, H2 |
| 32(1)(a), (b) | Security of processing for storage, transport and the command channel | C1, H3, M1 |
| 33(4) | Staged notification is expressly permitted if a breach is established | C1 |
| 35 | Impact assessment for a persistent identifier tied to a medical device | H2 |
| 37 | Data protection officer not found | Subject & Operator |

Whether any personal data was accessed through the key is not known. Whether a personal data breach occurred is for the controller to establish.

## Regulatory & Legal Landscape

The bases for this report are Regulation (EU) 2016/679 (GDPR) with Articles 5, 7, 9, 12, 13, 25, 32, 33, 35 and 37, and Regulation (EU) 2017/745 (MDR) Annex I Section 17.2. The disclosure follows ISO/IEC 29147 and rests on the freedom of research under Article 17 of the Austrian Staatsgrundgesetz.

The authorities named in the first notice as copied recipients are the Datenschutzbehörde (dsb@dsb.gv.at) and the European Data Protection Supervisor (edps@edps.europa.eu). The publication date is the date counted from delivery of the first notice.

## Indicators of Compromise & Reproducible Evidence

Every item below can be reproduced from the named APK. No server was authenticated against.

```
Package    com.ottobock.prosthetics.ll.cockpit 2.9.1.5 (20901005)
SHA-256    17e203c1b57dac6a47098a9f2fe24cafbf72fe036ec51ffac6df5650fe7a09b2
Cert (partial) 1ded03cf7a2df894cfcfb945627d77230a653ca8
Account    sampktsproduction  (blob.core.windows.net, 57.150.91.65)
DefaultEndpointsProtocol=https;AccountName=sampktsproduction;AccountKey=
    ekBOQwWDR6qEGf70tb9nvScZxGIQ7SkKqi8s2qVbl4GHSxfYK1kbiDKS/0MQA3049S8ZXB9y2VMt+AStho
    +ofQ==;EndpointSuffix=core.windows.net
Hosts      access/auth/consents/device/patients/profile/trial.swservice.ottobock.com
           mobileservice.ottobock.com/CockpitService.svc/json
           ob-environment.azurewebsites.net/api/  (NXDOMAIN)
           my.ottobock.com/info
BLE name   OB_(?<Type>.*?)(\[(?<BtVersion>[0-9])\])*_SN(?<Serial>[0-9]*)
Consent    /api/v1/consent/my  /api/v1/consent/accept  /api/v1/consent/terms
Policy     https://www.ottobock.com/media/local-media/sonstiges/cockpit-app/
    data_privacy.pdf  (307, 404)
```

Method: apktool decode of manifest and resources, a custom parser for the Xamarin assembly store (XABA container with LZ4-compressed XALZ assemblies), then UTF-16LE string extraction from the 123 decompressed assemblies. Passive checks were limited to DNS resolution and single unauthenticated HEAD requests.

## Disclosure Timeline & Outcome

| Date | Event |
|---|---|
| 22 Aug 2026 | First notice REF OTTOBOCKCOCKPIT-2026-R1 sent to cockpit@ottobock.com, myottobock@ottobock.com and info.austria@ottobock.com, with the Datenschutzbehörde and the EDPS in copy. Three questions asked. |
| 12 Sep 2026 | Follow-up to the same three addresses, three questions repeated word for word, answer requested by 26 Sep 2026. |
| 26 Sep 2026 | Deadline set in the follow-up. |
| 17 Oct 2026 | Second follow-up to the same three addresses with the open findings and the unchanged questions. |
| 15 Nov 2026 | Final notice from s.kepp@rfi-irfos.com to the same three addresses (14:09 UTC), titled 5 days to publication, naming 20 Nov 2026 as the publication date. |
| 20 Nov 2026 | Publication date, 90 days after the first notice. Embargo date reached. |
| 21 Nov 2026 | Report published. |

Outcome as of 21 November 2026: no substantive reply, no automatic acknowledgement and no bounce on any of the three addresses, including after the final notice of 15 November 2026.

## What Ottobock Got Right

SQLite storage is encrypted through SQLCipher and is not plaintext. Bluetooth and location permissions are scoped by Android version, with BLUETOOTH_SCAN carrying neverForLocation and location permissions requested only on the versions that need them. No advertising, attribution or session-replay SDK is present in any of the 123 assemblies, and the only telemetry is Microsoft App Center. No SDK or domain of a sanctioned or Chinese provider was found. targetSdkVersion 34 is maintained although feature development has stopped. A multilingual opt-in consent flow in 11 languages exists and is synchronised with a server-side consent API. No boot receiver and no content provider beyond the Mono bootstrap run before the user interface appears. The order of the App Center initialisation could not be determined from strings and is UNVERIFIED.

## Residual Risk & Recommendations

Rotating the storage account key closes C1 for every installed copy at once, because the embedded value becomes useless. Removing it from the next build is needed so that the new key is never embedded again. The other findings need changes on the device side and in the app.

| Priority | Action | Finding |
|---|---|---|
| 1 | Rotate the account key of sampktsproduction and review account logs | C1 |
| 2 | Stop embedding account keys in client code, use read-only scoped access | C1 |
| 3 | Document authentication and integrity controls on the file commands | H3 |
| 4 | Replace the identifying device name with a rotating identifier | H2 |
| 5 | Add in-app consent withdrawal using the existing API | M2 |
| 6 | Restore the privacy document and name a data protection officer | M3 |
| 7 | Add pinning, retire unused hosts, migrate the UI framework | M1, H1, M4 |

Residual risk: all copies of version 2.9.1.5 already distributed keep the embedded key. This report describes version 2.9.1.5 only.

**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 passive public DNS and HTTP HEAD requests. No Ottobock servers or accounts were probed and the extracted key was never used. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Arts. 5, 7, 9, 12, 13, 25, 32, 33, 35, 37, MDR (EU) 2017/745 Annex I Section 17.2. RFI-IRFOS ZVR 1015608684, GISA 39261441. REF OTTOBOCKCOCKPIT-2026-R1.