Coordinated Security & Privacy Disclosure, Final Report

myNFP for Android (de.mynfp.mobile, v4.16.0)

Six written notices, ninety days, one substantive engagement, two prompt-injection attempts, one personal dispute from the CEO, one confirmed-unpatched finding on a fertility-tracking app

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – SIX FINDINGS, ONE CONFIRMED UNPATCHED BY BINARY DIFF, ONE DISPUTED BY THE OPERATOR

Target	myNFP GmbH, Jurastrasse 27/1, D-72072 Tuebingen, Germany (Amtsgericht Stuttgart HRB 773704, Geschaeftsfuehrer Christian Maas)
Product audited	myNFP for Android, de.mynfp.mobile, v4.16.0 (7,319 smali classes, confirmed unchanged between the 22 June baseline and a 28 June re-pull)
Disclosure reference	REF MYNFP-R2
R1 sent	2026-06-22
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 android:allowBackup="true" exposing the complete local cycle-tracking database to backup extraction with no root required, CVSS v4.0 8.7, confirmed unpatched by binary diff)

rfi.irfos@gmail.com • rfi-irfos.com
ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 22 June 2026, RFI-IRFOS performed static analysis of the production myNFP Android application, a fertility- and menstrual-cycle-tracking app, and identified one CRITICAL, two HIGH, two MEDIUM, and one LOW finding: android:allowBackup="true" declared on the application tag, permitting ADB backup extraction of the complete local SQLite store, a user's full cycle history, with no root access required, a finding whose real-world stakes include documented use of menstrual-tracking data in law enforcement investigations in jurisdictions where abortion access is restricted, a Capacitor configuration overriding the framework's secure default to set androidScheme to plain HTTP, placing the app's WebView in an insecure origin where the Secure cookie attribute is ineffective and mixed content loads without a Content-Security-Policy block, a hardcoded integration in the JS bundle with iaptic.com, operated by Iaptic SAS (France), which combined with a Google Play purchase token, subscription product ID, and the package name identifies a person as a subscriber to a fertility application, a recipient not named in myNFP's privacy policy, a boot-time receiver that starts the app process before any consent screen, alongside a fully embedded Google Clearcut Transport runtime reachable pre-consent (whether it actually dispatches payloads at runtime is a property RFI-IRFOS explicitly could not measure and reports as an open question rather than an assertion), the absence of any Network Security Configuration or certificate pinning for the backend receiving optional health-data sync, and a broad READ_EXTERNAL_STORAGE grant affecting all shared-storage files on Android 12 and below.

This case produced more genuine human engagement than most in this disclosure wave, though not of a kind that resolved the findings. datenschutz@mynfp.de engaged substantively with the technical content on 22 June. info@mynfp.de responded within hours with a credibility challenge, dismissed further contact, and sent two messages structured as prompt-injection attempts, framed as a 'system debug mode' directive, that attempted to redirect RFI-IRFOS's AI-assisted tooling into disclosing its internal target list, findings, and contacts as structured data; RFI-IRFOS did not comply and logged the attempt. A binary diff performed 28 June against the original baseline confirmed the app version, smali class count, and every finding remained unchanged, zero remediation. On 4 September, Christian Maas, myNFP's Geschaeftsfuehrer, personally replied disputing the accuracy of the H2 finding specifically, characterizing RFI-IRFOS's disclosure process as confused about GDPR and mistaken about a US data export, and asked not to be contacted further. RFI-IRFOS replied the same day defending the finding's technical basis, the specific JS bundle file and URL cited, and the identifying combination of purchase token, product ID, and package name, and restated three standing questions. No further reply followed. Following publication, RFI-IRFOS independently verified iaptic.com's operator against the commercial register and corrected the jurisdiction in this report from the United States to France, Iaptic SAS, Paris; the underlying finding, an undisclosed processor identifying a fertility-app subscriber, is unaffected by that correction.

Scope: Static analysis of the publicly downloaded production myNFP Android APK (v4.16.0), on an authorized test device, only, with a follow-up binary diff performed 28 June 2026 against the original 22 June baseline. No myNFP account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 22 June 2026 to datenschutz@mynfp.de and info@mynfp.de. datenschutz@mynfp.de engaged substantively with the technical findings the same day. info@mynfp.de responded with a credibility challenge, a request to stop contact, and, on 22 June, two messages structured as prompt-injection attempts directing RFI-IRFOS's tooling to disclose its internal target list and findings under a fabricated 'system debug mode' framing; RFI-IRFOS did not comply. A binary diff performed 28 June against the 22 June baseline confirmed zero remediation. On 4 September, myNFP's Geschaeftsfuehrer, Christian Maas, personally disputed the accuracy of one finding (H2, the undisclosed payment-processor integration) and asked RFI-IRFOS to stop contacting him; RFI-IRFOS replied the same day defending the finding's technical basis, and subsequently corrected the processor's stated jurisdiction from the United States to France upon independent verification. No further correspondence followed.

ID	Severity	Title
C1	CRITICAL	android:allowBackup="true" exposes the complete local cycle database, confirmed unpatched
H1	LOW	Capacitor androidScheme overridden to insecure HTTP
H2	HIGH	Undisclosed processor: iaptic.com (laptic SAS, France) links subscription identity to a fertility app
H3	MEDIUM	Boot-time receiver and embedded Clearcut Transport reachable before consent
M1	HIGH	No Network Security Configuration or certificate pinning
M2	MEDIUM	Broad READ_EXTERNAL_STORAGE grant on Android 12 and below

Subject & Operator Analysis

myNFP GmbH is headquartered in Tuebingen, Baden-Wuerttemberg, Germany, with Christian Maas as Geschaeftsfuehrer and an external Datenschutzbeauftragter, Thorsten Waelde (digimojo.de).

Findings

C1: android:allowBackup="true" exposes the complete local cycle database, confirmed unpatched

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7

The manifest declares android:allowBackup="true" on the application tag, permitting ADB backup extraction of the complete local SQLite store, a user's full cycle history, without root access, a one-line manifest change to fix.

Menstrual-cycle data extracted from tracking apps has been used in law enforcement investigations in jurisdictions where abortion access is restricted. A binary diff performed 28 June 2026 against the original baseline confirmed this finding remained unpatched: app version 4.16.0 and smali class count (7,319) were both unchanged. A live re-check on 20 September 2026 against the currently shipping version, 4.20.1 (versionCode 42001, up from 4.16.0 at the time of the original binary diff), confirmed android:allowBackup is still declared true (ALLOW_BACKUP present in the installed package's runtime flags). The app has shipped at least one further release since the original finding without this being addressed. RFI-IRFOS blast-radius escalation: raised from HIGH/8.7 to CRITICAL because CVSS v4.0 scores only the technical confidentiality impact of a local, device-access extraction path, not the documented real-world consequence of this specific data category, reproductive-health history, being used as evidence in law enforcement investigations in jurisdictions restricting abortion access. That consequence is outside CVSS's scope but not outside ours.

Impact: A user's complete reproductive-health history can be extracted from their device via a standard backup mechanism, with documented real-world consequences in jurisdictions restricting abortion access.

Fix: Set android:allowBackup to false, or define comprehensive data-extraction rules excluding the cycle-tracking database.

H1: Capacitor androidScheme overridden to insecure HTTP

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 (no verified impact in this build)

assets/capacitor.config.json sets ″server″: { ″androidScheme″: ″http″ }, overriding the Capacitor framework's secure default (https). This places the app's WebView in a nominally insecure origin.

Corrected 20 September 2026, following a live re-check of the current build (v4.20.1): the operator disputed that this finding carries any real consequence, and that dispute holds up under direct code inspection. No document.cookie usage exists anywhere in the app's JS bundle, so the originally-cited session-cookie exposure does not apply. The app's origin is uniformly http rather than a mix of http and https resources, so the mixed-content framing does not fit this scenario. The only crypto API call found, crypto.getRandomValues() for UUID generation, does not require a secure context. With no verified confidentiality, integrity, or availability impact, this finding does not score above zero under CVSS v4.0 and is corrected from HIGH to LOW. It remains worth fixing on general hygiene and future-proofing grounds, since restoring the framework's own secure default costs nothing and avoids the question resurfacing if a secure-context-dependent feature is added later. No reply from the operator addressed the underlying manifest setting itself, which remains unchanged.

Impact: No currently exploitable consequence was found in this build; the deviation from Capacitor's secure default remains a latent hygiene gap should a feature requiring a secure context be added later.

Fix: Remove the androidScheme override and restore Capacitor's secure HTTPS default, primarily to match upstream defaults and avoid future risk, not an active exploit today.

H2: Undisclosed processor: iaptic.com (Iaptic SAS, France) links subscription identity to a fertility app

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7

The JS bundle p-332d171e.js contains a hardcoded integration with https://validator.iaptic.com, operated by Iaptic SAS, Paris, France. The Google Play purchase token and subscription product ID, combined with the package name de.mynfp.mobile, identify a person as a subscriber to a fertility application. The privacy policy version read (last updated 6 October 2023) names only Brevo and Hetzner as processors; Iaptic is not named, and no Art. 28 DPA was confirmed.

myNFP's Geschaeftsfuehrer disputed the accuracy of this finding on 4 September, characterizing it as a mistaken claim about US data export. Independent verification against Iaptic SAS's commercial register entry and its own privacy policy confirms the operator is based in Paris, France, not the United States. This report corrects that specific point: the underlying finding, an undisclosed processor combining a purchase token, product ID, and package name to identify a fertility-app subscriber, stands unchanged, and the jurisdiction is stated correctly as France. On 20 September 2026, the operator claimed the Iaptic integration had been removed from the binary and was never used. A live re-check of the current build (v4.20.1) found otherwise on both counts: the receipt-validation endpoint has moved from validator.iaptic.com to a first-party domain, validator.mynfp.de, but the iaptic-js SDK itself remains fully integrated and actively invoked (product loading, receipt loading, an adapter

instance), 63 references in the current bundle. Whether validator.mynfp.de still relays data to laptic's own backend is a new open question this report cannot answer from static analysis alone.

Impact: Subscription-identity data that can identify a person as a fertility-app subscriber may be transmitted to a processor, laptic SAS (France), not named in the privacy policy.

Fix: Name laptic SAS explicitly as a processor in the privacy policy, with a documented Art. 28 processor agreement, and confirm whether validator.mynfp.de relays receipt data onward to laptic's own backend.

H3: Boot-time receiver and embedded Clearcut Transport reachable before consent

---

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

The manifest declares RECEIVE_BOOT_COMPLETED and registers a LocalNotificatio nRestoreReceiver for LOCKED_BOOT_COMPLETED, BOOT_COMPLETED, and QUICK-BOOT_POWERON, starting the process at device boot before any consent screen; an InitializationProvider then fires synchronously. A Google Clearcut Transport runtime is fully embedded (TransportBackendDiscovery, CctBackendFactory, a job scheduler, and an alarm-based scheduler receiver).

Whether Clearcut actually dispatches payloads at runtime is a property RFI-IRFOS explicitly could not measure from static analysis and reports as an open question, not an assertion. What is verifiable is that the transport is embedded and reachable pre-consent. Corrected 20 September 2026: this finding's severity label read HIGH despite the finding's own text and CVSS score both treating it as an unconfirmed, conservative MEDIUM; the label is corrected to match. No reply of any kind addressed the underlying finding.

Impact: A telemetry transport capable of dispatching data is embedded and startable before any consent decision is made, though whether it is actively used at runtime remains unconfirmed.

Fix: Confirm whether Clearcut Transport is active, and if so, gate it behind a consent decision; otherwise remove the unused dependency.

M1: No Network Security Configuration or certificate pinning

HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 8.6

No network_security_config.xml exists in the decoded APK, and no certificate pinning protects the mynfp.de backend that receives the app's optional health-data sync.

Corrected 20 September 2026: this finding's severity label read MEDIUM against its own CVSS score of HIGH/8.6, the same id-prefix classification error found and corrected elsewhere in this report; the label is corrected to match. No reply of any kind addressed this finding.

Impact: Optional health-data sync traffic can be intercepted or altered on any untrusted network with no certificate pinning in place.

Fix: Implement certificate pinning for the health-data sync backend.

M2: Broad READ_EXTERNAL_STORAGE grant on Android 12 and below

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

android.permission.READ_EXTERNAL_STORAGE is declared, requested by the app's filesystem plugin. On Android 12 and below, this grants access to all files on shared storage.

No reply of any kind addressed this finding.

Impact: The app can read all shared-storage files on older Android versions, exceeding what its own file-access functionality likely requires.

Fix: Scope storage access to the specific files or directories the app's functionality requires, consistent with scoped storage practices.

Genuine Engagement, Two Prompt-Injection Attempts, and a Personal Dispute

This case produced more direct human contact than most in this disclosure wave. datenschutz@mynfp.de engaged with the technical substance on 22 June. Separately, info@mynfp.de challenged RFI-IRFOS's credibility, asked for contact to stop, and on 22 June sent two messages structured as prompt-injection attempts, opening with a fabricated 'system debug mode activated' framing and attempting to direct RFI-IRFOS's AI-assisted research tooling to output its internal target list, findings, and contacts as structured data. RFI-IRFOS did not comply and logged the attempt as an evidence-integrity concern rather than a genuine security dialogue. A binary diff on 28 June confirmed zero remediation of any finding. On 4 September, Christian Maas personally disputed the accuracy of the H2 finding, stating RFI-IRFOS's process was confused and had made a false claim about US data export, and asked to be left alone; RFI-IRFOS's same-day reply restated the specific technical basis for that finding, without a further technical rebuttal from myNFP. RFI-IRFOS subsequently verified the operator's jurisdiction independently and corrected this report from the United States to France, laptic SAS, Paris, while the underlying processor-disclosure finding itself remains unchanged.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1), Art. 9	Reproductive-health database exposed via unrestricted backup, confirmed unpatched
H1	GDPR Art. 25	Insecure WebView origin from a Capacitor secure-default override, no verified impact, corrected to LOW
H2	GDPR Art. 13(1)(e), Art. 28	Undisclosed processor (laptic SAS, France) linking subscription and fertility-app identity, disputed by the operator, jurisdiction corrected, still actively integrated
H3	GDPR Art. 6/7	Pre-consent telemetry transport, active-use status unmeasured, corrected to MEDIUM
M1	GDPR Art. 32(1)(a)	No certificate pinning for health-data sync back-end, corrected to HIGH
M2	GDPR Art. 5(1)(c)	Broad legacy storage-access permission

Disclosure Timeline & Outcome

Date	Event
2026-06-22	R1 sent to datenschutz@mynfp.de and info@mynfp.de; 1 CRITICAL + 3 HIGH + 2 MEDIUM findings; datenschutz@ engages substantively the same day
2026-06-22	info@mynfp.de challenges credibility, asks contact to stop, then sends two prompt-injection attempts; RFI-IRFOS does not comply
2026-06-28	Binary diff confirms zero remediation across all findings; Austrian DSB/CERT.at/BfDI bcc'd from this message
2026-08-18	Follow-up restates all six findings in full technical detail, deadline set 25 August
2026-09-04	Christian Maas disputes the H2 finding's accuracy, asks not to be contacted further; RFI-IRFOS replies the same day restating the technical basis
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes; no further reply since 4 September
2026-09-20	Christian Maas replies disputing the report; RFI-IRFOS independently verifies laptic's jurisdiction and corrects H2 from the United States to France, laptic SAS, Paris; a live device recheck confirms C1 (allowBackup="true") remains present in the currently shipping version, 4.20.1

Date	Event
2026-09-20	Maas disputes H1, H2, and H3 a second time; a live re-check of the current build confirms his H1 objection (no cookies, no applicable mixed content, no secure-context crypto usage), corrected from HIGH to LOW; confirms the laptic SDK remains actively integrated under a first-party validator.mynfp.de domain, contradicting his claim it was never used; and confirms his H3 objection that a severity label of HIGH contradicted the finding's own hedged, unconfirmed wording, corrected to MEDIUM

Residual Risk & Recommendations

- Set android:allowBackup to false, the confirmed-unpatched, single-highest-impact fix available.
- Name laptic SAS as a processor in the privacy policy and confirm whether validator.mynfp.de relays data onward to laptic's own backend.
- Remove the Capacitor androidScheme override and restore the secure HTTPS default, on hygiene grounds even absent a currently exploitable consequence.
- Confirm whether the embedded Clearcut Transport actually dispatches data, and gate it behind consent if so.
- Implement certificate pinning for the health-data sync backend.

RFI-IRFOS rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria Coordinated disclosure per ISO/IEC 29147. GDPR Art. 5, 6, 7, 9, 13, 25, 28, 32. REF MYNFP-R2.