Coordinated Security & Privacy Disclosure, Final Report

DaysyDay for Android (ch.valleyelectronics.daysyday)

Twelve written notices, ninety-one days, three dead or dying contact addresses, one automated ticket acknowledgment, zero substantive replies, reproductive health data at issue throughout

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – SEVEN FINDINGS ON A FERTILITY-TRACKING APP, INCLUDING UNDISCLOSED ART. 9 DATA ROUTED TO THE US

Target	Valley Electronics AG (”Valley Company”); M.I.S.S. GmbH, Breite 2, 82418 Murnau a. Staffelsee, Germany (Registergericht München HRB 77457, Geschäftsführung Collin Egly) operates the daysy.me support brand; Milk Interactive AG, Brauerstrasse 126, Zürich, is an undisclosed third-party developer/processor identified in the APK
Product audited	DaysyDay for Android, ch.valleyelectronics.daysyday, v1.5.4
Disclosure reference	REF: ch.valleyelectronics.daysyday
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	HIGH (C1 hardcoded Sentry DSN exposing fertility-app crash breadcrumbs, CVSS v4.0 8.8; C2 Art. 9 sexual-activity and fertility data routed to a US endpoint with no disclosed transfer mechanism, CVSS v4.0 8.7, both unaddressed)

rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production DaysyDay Android application, a Bluetooth basal-thermometer companion app for fertility tracking, and identified seven findings: a hardcoded Sentry DSN whose crash-report breadcrumbs, in a fertility tracker, carry reproductive health context and are sent to an undisclosed recipient; a production endpoint (usa.daysy.measur) routing cycle, ovulation, and sexual-activity data, extracted verbatim from the app’s own bundled strings, to the United States with no disclosed transfer mechanism, directly contradicting the app’s own privacy policy claim that data stays in Switzerland and Germany; GPS and microphone permissions with no fertility-tracking use case and no privacy-policy disclosure; a production Network Security Config permitting unencrypted HTTP traffic to a public, non-private IP address; an undisclosed third-party developer, Milk Interactive AG of Zürich, whose package namespace retains production database-migration access to fertility records with no Art. 13(1)(e) or Art. 28 disclosure; a self-hosted Matomo analytics instance tracking feature usage on an Art. 9 health platform with no documented special-category legal basis; and a minimum Android platform baseline of 7.0 (2016), disproportionate to the real-world employment, insurance, and, in some jurisdictions, legal consequences a breach of reproductive health data can carry.

This case’s delivery record deteriorated over its course. R1 was sent to the two daysy.me support addresses; a follow-up cc to press@valleyelectronics.ch bounced immediately (the domain no longer resolves), and info@ch.daysy.me began rejecting RFI-IRFOS’s mail as spam from the second message onward. By 4 August 2026, info@eu.daysy.me also began rejecting RFI-IRFOS’s mail, leaving both original contact addresses dead; RFI-IRFOS switched on 12 August 2026 to hello@valley-company.com, Valley Electronics AG’s own published address, restating the two CRITICAL and the Milk Interactive findings. That address also never substantively replied. The only inbound message across all three threads and the full ninety-one-day period was a single automated, five-language ticket acknowledgment (case #607063, 17 July 2026), confirming receipt and linking an FAQ page.

None of the six standing questions, on the US-transfer contradiction, whether Milk Interactive AG is bound as an Art. 28 processor, and whether the Austrian DSB, the EDÖB, or a lead supervisory authority was notified under Art. 33 within 72 hours, or whether an Art. 35(3)(b) DPIA was conducted for this large-scale Art. 9 processing, ever received an answer. For transparency: R1’s own body text stated that the EDÖB, the Austrian DSB, and BayLDA (M.I.S.S. GmbH’s regulator) were in bcc on that message; RFI-IRFOS’s own sent-message record shows R1’s actual bcc field did not include those regulator addresses, an internal inconsistency corrected from the 27 June 2026 follow-up onward, where dsb@dsb.gv.at, cert@cert.at, and poststelle@bfdi.bund.de were genuinely cc’d or bcc’d throughout.

Scope: Static analysis of the publicly downloaded production DaysyDay Android APK (v1.5.4), including Hermes bytecode string extraction from assets/index.android.bundle, on an authorized test device, only. No DaysyDay account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 20 June 2026 to info@ch.daysy.me and info@eu.daysy.me. Across twelve written notices over ninety-one days, spanning three Gmail threads, both original daysy.me contact addresses stopped accepting mail entirely, forcing a channel switch on 12 August 2026 to hello@valley-company.com, Valley Electronics AG’s own published address, which likewise never substantively replied. The only inbound message across the entire case was a single automated, five-language support-ticket acknowledgment on 17 July 2026, pointing to an FAQ page. No RFI-IRFOS finding or question was ever answered by a named person.

ID	Severity	Title
C1	HIGH	Hardcoded Sentry DSN exposes fertility-app crash breadcrumbs
C2	HIGH	Sexual-activity and fertility data routed to a US endpoint, contradicting the app’s own privacy policy
H1	MEDIUM	Location and microphone permissions with no fertility-tracking use case
H2	HIGH	Cleartext HTTP permitted to a public IP in the production Network Security Config
H3	MEDIUM	Milk Interactive AG, undisclosed developer with production database-migration access
H4	MEDIUM	Matomo behavioral analytics on an Art. 9 health platform, no documented legal basis
H5	LOW	minSdk 24 (Android 7.0, 2016), disproportionate for reproductive health data

Subject & Operator Analysis

Three distinct entities are involved and are kept separate throughout this report: Valley Electronics AG (”Valley Company”), the app’s publisher and this disclosure’s current outreach target; M.I.S.S. GmbH, Breite 2, 82418 Murnau a. Staffelsee, Germany (Registergericht München HRB 77457, Geschäftsführung Collin Egly), which operates the daysy.me support brand and issued the case’s only reply, an automated ticket acknowledgment; and Milk Interactive AG, Brauerstrasse 126, Zürich, an undisclosed third-party developer identified in finding H3, not itself a disclosure recipient.

Findings

C1: Hardcoded Sentry DSN exposes fertility-app crash breadcrumbs

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 8.8

A full Sentry DSN credential, https://d596f29f7218450fa75ee20f62cca78c@sentry2.daysy.me/4, is hardcoded verbatim in assets/index.android.bundle (Hermes bytecode), extractable from any downloaded APK in under 60 seconds.

Sentry captures session breadcrumbs at crash time; in a fertility tracker, that breadcrumb trail carries reproductive health context. sentry2.daysy.me is not named as a data recipient anywhere in the app’s privacy documentation. Never addressed across twelve notices.

Impact: Crash-time session context for a reproductive-health app is sent to an undisclosed recipient, and the extracted DSN itself could be used to submit forged events into the project’s crash stream.

Fix: Rotate the DSN, restrict it via Sentry’s own key-scoping controls, and name sentry2.daysy.me explicitly as a data recipient in the privacy policy.

C2: Sexual-activity and fertility data routed to a US endpoint, contradicting the app’s own privacy policy

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 production bundle contains three regional endpoints, ch.daysy.measur, eu.daysy.measur, and usa.daysy.measur. Verbatim bundle strings confirm the US endpoint carries cycle data, ovulation records, and sexual-activity logs (”Average length of luteal phase”, ”Type de rapports sexuels”, ”E_PARTNER_REMOVED”, ”DaysyDayLogs.txt”).

The app’s own privacy policy states data is held on ”secured servers in Switzerland and Germany”, directly contradicted by this endpoint’s existence. No Standard Contractual Clauses or equivalent Art. 44-49 transfer mechanism is disclosed. Two direct yes/no questions on this contradiction were asked repeatedly and never answered.

Impact: Art. 9 special-category reproductive and sexual-activity data reaches a US endpoint with no disclosed lawful transfer basis, directly contradicting the data-residency claim users are shown.

Fix: Either remove the usa.daysy.measur endpoint from EU/CH user data flows, or disclose it explicitly with a valid Art. 44-49 transfer mechanism and correct the privacy policy’s residency claim.

H1: Location and microphone permissions with no fertility-tracking use case

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

ACCESS_FINE_LOCATION and RECORD_AUDIO are present on a Bluetooth basal-thermometer companion app; neither is required for temperature tracking, cycle logging, or ovulation prediction.

Location data could geolocate intimate health events. Neither permission is mentioned or justified anywhere in the privacy documentation. Never addressed in the case’s only reply.

Impact: Two sensitive device capabilities are granted on a reproductive-health app with no documented purpose, exceeding the data-minimization principle for Art. 9 processing.

Fix: Remove ACCESS_FINE_LOCATION and RECORD_AUDIO unless a specific, disclosed feature requires them.

H2: Cleartext HTTP permitted to a public IP in the production Network Security Config

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

The production (non-debug-overrides) Network Security Config permits unencrypted traffic to 192.160.101.1, a public, non-private IP address.

Not disclosed anywhere in the app’s privacy or security documentation. Never addressed across twelve notices.

Impact: On an adjacent, attacker-controlled network, fertility and health data transmitted to this address can be intercepted or manipulated in plaintext.

Fix: Remove the cleartext exception for this address and enforce TLS for all production traffic.

H3: Milk Interactive AG, undisclosed developer with production database-migration access

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.9

The manifest declares ch.milkinteractive.daysyday.datamigrationprovider.CONTENT_PROVIDER. Milk Interactive AG (Brauerstrasse 126, Zürich) built the app, and its package namespace remains in the production binary with database-migration access to fertility records.

Milk Interactive is not named as a data processor or recipient in the privacy policy. Whether it is contractually bound as an Art. 28 processor was asked on 12 September 2026 and never answered.

Impact: An undisclosed third-party developer retains production-level database migration access to Art. 9 reproductive health records with no confirmed Art. 28 processor agreement or Art. 13(1)(e) disclosure.

Fix: Name Milk Interactive AG explicitly as a processor with its Art. 28 agreement referenced in the privacy policy, or remove its production access if the engagement has ended.

H4: Matomo behavioral analytics on an Art. 9 health platform, no documented legal basis

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

A self-hosted Matomo instance at matomo.daysy.me tracks feature usage, screen views, and session frequency.

When ovulation data is entered and which cycle features are accessed are themselves health-adjacent Art. 9 signals; legitimate interest does not provide a lawful basis for special-category data. The specific endpoint and its Art. 9 context are not individually disclosed under Art. 13(1)(c). Never addressed.

Impact: Usage-pattern analytics on a fertility app can itself constitute special-category data processing operating without a documented Art. 9(2) legal basis.

Fix: Document an Art. 9(2) legal basis for this analytics processing, or restrict Matomo from collecting events tied to reproductive-health feature usage.

H5: minSdk 24 (Android 7.0, 2016), disproportionate for reproductive health data

LOW, CVSS v4.0 AV:A/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 2.3

The app supports Android 7.0 (API 24), a platform baseline ten years old at time of disclosure.

A breach of this data profile, cycles, fertility windows, sexual activity, pregnancy planning, carries real-world consequences in employment, insurance, and in some jurisdictions legal jeopardy. GDPR Art. 32 requires security measures proportionate to this risk. Never addressed.

Impact: The oldest supported devices lack current platform security mitigations for data whose exposure carries unusually high real-world consequence for the individuals affected.

Fix: Raise minSdk in line with a risk-proportionate security baseline for Art. 9 reproductive health data.

Two Dead Addresses and a Channel Switch

This case’s delivery record deteriorated in real time. info@ch.daysy.me began rejecting RFI-IRFOS’s mail as spam from the second notice onward; a cc to press@valleyelectronics.ch bounced immediately because the domain no longer resolves. info@eu.daysy.me remained reachable and even generated the case’s only reply, an automated ticket acknowledgment on 17 July 2026, but itself began rejecting RFI-IRFOS’s mail as spam from 4 August 2026. RFI-IRFOS switched on 12 August 2026 to hello@valley-company.com, Valley Electronics AG’s own published contact, restating the CRITICAL findings and the Milk Interactive question; that address never substantively replied either, across five further notices through 12 September 2026.

A Correction on Our Own Record

For transparency: R1’s own body text stated that the EDÖB, the Austrian DSB, and BayLDA were in bcc on that message. RFI-IRFOS’s own sent-message record for R1 does not show those regulator addresses in the actual bcc field. This discrepancy is documented here rather than left implicit; genuine cc/bcc to dsb@dsb.gv.at, cert@cert.at, and poststelle@bfdi.bund.de begins from the 27 June 2026 follow-up onward and continues throughout the remainder of the case.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 13(1)(e), Art. 32	Undisclosed crash-reporting recipient exposing health-adjacent breadcrumbs
C2	GDPR Art. 9, Art. 44-49, Art. 13(1)(f)	Reproductive/sexual-activity data to a US endpoint, no disclosed transfer mechanism, contradicts stated data residency
H1	GDPR Art. 5(1)(c), Art. 13(1)(c)	Location/microphone permissions with no disclosed fertility-tracking use case
H2	GDPR Art. 32(1)(a)	Cleartext HTTP to a public IP in production
H3	GDPR Art. 13(1)(e), Art. 28	Undisclosed processor with production database-migration access
H4	GDPR Art. 9(2), Art. 13(1)(c)	Behavioral analytics on Art. 9 platform, no documented legal basis
H5	GDPR Art. 32	Disproportionate minimum platform baseline for Art. 9 data’s risk profile

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to info@ch.daysy.me and info@eu.daysy.me; 2 CRITICAL + 5 HIGH findings; embargo set to 2026-09-19
2026-06-27	Follow-up, cc press@valleyelectronics.ch bounces (NXDOMAIN); info@ch.daysy.me rejects as undeliverable
2026-06-28	Follow-up, info@ch.daysy.me bounces with a 554 5.7.1 spam rejection
2026-07-04	Follow-up sent to info@eu.daysy.me only, embargo and findings restated
2026-07-17	Follow-up sent; same day, the case’s only inbound reply arrives, an automated five-language ticket acknowledgment, case #607063
2026-07-27	Follow-up, day 10 since the only reply, three questions repeated
2026-08-04	Follow-up bounces: info@eu.daysy.me now also rejects as spam, both original daysy.me addresses dead
2026-08-12	Channel switch to hello@valley-company.com, cc regulators, C1/C2/H3 restated
2026-08-18	Follow-up, day 59, new deadline set for 25 August 2026
2026-09-01	Follow-up, day 73, 25 August deadline passed with no reply
2026-09-04	Follow-up, day 76, new deadline set for 11 September 2026
2026-09-12	Follow-up, day 84, 11 September deadline passed with no reply; full chronology and six questions restated; embargo reconfirmed fixed regardless of reply
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Rotate the exposed Sentry DSN and name it explicitly as a data recipient in the privacy policy.
- Remove or properly disclose the usa.daysy.measur endpoint and correct the privacy policy’s data-residency claim.
- Remove location and microphone permissions absent a specific, disclosed use case.
- Enforce TLS for all production traffic and remove the public-IP cleartext exception.
- Name Milk Interactive AG explicitly as a processor with a referenced Art. 28 agreement, or remove its production access.
- Document an Art. 9(2) legal basis for behavioral analytics tied to reproductive-health feature usage.
- Fix an operational support channel that stops rejecting inbound mail as spam, so future user and regulator correspondence is not silently lost.

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. Research activity protected under Austria’s Forschungsfreiheitsgesetz (Art. 17 StGG). GDPR Art. 5, 9, 13, 28, 32, 33, 35, 44-49. REF ch.valleyelectronics.daysyday.