TALIA: Menopause & HRT Tracker

Type: iOS
Version: 1.1.1
Latest release: 10 Jun 2026
Publisher: Create West Country Ltd

PEAK PRIVACY GOLD VERIFIED PPCS v1.0 TALIA: Menopause & HRT Tracker v1.1.1 · 10 Jun 2026

Your data goes to no one but the app's own service. No third parties, no tracking, no hidden identifiers.

Reassessed on every new release.

TIER · GOLD

0 Other companies your data was sent to

0 Hidden IDs that can track you

POLICY VS BEHAVIOUR

WHAT THEY CLAIM		WHAT THE EVIDENCE SHOWS
No third parties named in the policy	0 UNDISCLOSED	No third parties observed
0		0

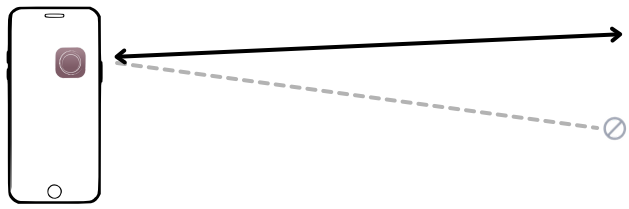
CONSENT

Does the app need to ask for informed consent, if so, does the app ask for consent correctly? Does the consent solution block trackers and network calls when consent is denied?

Consent Banner Required	Consent Banner Existing	Consent Banner Correct	Consent Banner Working
NO	NO	–	–

WHERE YOUR DATA GOES

Talia contacts one place. Talia sends no data to third parties.



Your phone

Own services - no personal data sent
talia-app.com · for update checks · no personal data sent

Third party services - nothing sent
Adtech · Analytics · Other apps, etc.

WHAT, WHERE AND WHAT KIND?

Every "place" the app connected to during the test. TALIA made just one connection, to its own server, to check for an update.

Destination	Type	Sever Location	Vendor Jurisdiction	What was sent	Third Party SDK*
talia-app.com/app-version.json	First party	United Kingdom	United Kingdom	App update check - no personal data	No

*Software Development Kit. Ready-made code from another company, built into an app. "No" means the connection came from the app's own code, not through a ready made externally sourced SDK.

PERMISSIONS

The features of the phone an app can reach, camera, location, health, contacts, and so on. We check whether every feature it asks for is needed for what the app does: green means yes, necessary; amber or red means it asks for more than it should. A permission is only as risky as where the data can go, so read this alongside the connections table above. A camera permission on an app that sends nothing out is harmless; the same permission next to advertising SDKs is not.

Permission	What the app says it is for	Necessary for the apps purpose
—	—	—

Methodology

Standard	· Peak Privacy Certification Standard, version 1.0
Method	· Dynamic testing of the published app. An automated agent exercises the app for ~1.5 minutes, capturing every network call, identifier and permission. Identical for every app.
Monitoring	· Re-assessed on every new release. The tier moves if the behaviour moves.
Independence	· A certificate is earned, never bought. Peak Privacy issues it only when the scan meets the standard, and withdraws it when a release no longer does.
Oversight	· Our methodology is published in full and open to independent review. Every certificate is publicly verifiable against its evidence at stemp.li.
Issuer	· Peak Privacy ApS, Copenhagen, Denmark, The European Union | CVR 45354059 | Certificate can not be issued by Peak Privacy if the test result does not live up to the result

HOW TO READ THIS CERTIFICATE

This record explains what was tested and what it means for the people who use the app. It is the full record for a certified app; apps without a tier show the summary only. The sections below define each variable and why it appears.

Legal framework

Apps are assessed against European privacy law: the General Data Protection Regulation (GDPR) and the ePrivacy rules, as implemented across the EU and EEA. Two questions sit behind every result. First: did the app store or read anything on your device that wasn't strictly necessary, without your consent? Second: is any personal data it processes handled lawfully, transparently, and only as far as needed? Some data, health, sexual life, religion and similar, is "special category" data and carries stricter rules.

Testing method

The published app is run dynamically by an automated agent for about 1.5 minutes, recording every connection, identifier and permission. Identical for every app. Findings are detected, not self-declared.

Consent

European privacy law requires an app to ask for your consent before it stores or reads anything on your device that isn't strictly necessary, like advertising, analytics etc. Things you asked for, like signing in or paying, don't need consent. The four checks read in order: **Required,** whether the app does anything that needs consent at all ("No" means everything it does is strictly necessary); **Existing,** whether a consent banner is actually present; **Correct,** whether that banner is built properly, with a genuine choice and a reject option as easy as accept; **Working,** whether refusing consent actually stops the trackers and network calls. A "No / No" on the first two is a strong result, not a gap. A dash means "not applicable", there's no banner to assess. The last check catches the most: a banner that exists but doesn't stop tracking when you decline gives the appearance of consent without the substance, and is treated as a failure.

Connections and data transfer

"First-party" is the app's own service; "third-party" is another company. An IP address is personal data, and one is exchanged on every connection, a server can't reply without seeing your address, so its presence alone is not a sign of tracking. What matters is whether anything beyond that is sent, to whom, whether it was needed, and whether the destination simply uses the address to answer the request or retains it to build a profile. Two things about *where* then matter, and they can differ. Server location is where the destination server physically answered from. Vendor jurisdiction is the legal home of the company that controls it and that is what governs the data, because a server in Germany operated by a US company such as Amazon or Google is still reachable by US law. EU soil does not mean EU control. When personal data leaves the EU/EEA, or stays on EU soil but under non-EU control, GDPR requires equivalent protection (an adequacy decision, or specific safeguards). This report flags where data went and whose jurisdiction applies; it does not rule on whether that safeguard is in place.

Identifiers and profiling

Some things act as a name tag for your device or your activity in the app: an advertising identifier, a cookie or other stored marker, or a "fingerprint" assembled from your device's characteristics. The report records when these are placed on your device or sent to another company. On their own they can look harmless, but they are the raw material of profiling — they let a company recognise your device and combine its activity with data from other sources.

Permissions

The phone features an app declares it can reach, each judged against whether it's necessary for the app's stated purpose. Granting a permission is a technical setting, not legal consent. A permission only matters in proportion to what can leave the device, so it's read alongside the connections above.

Tiers

Gold, Silver and Bronze reflect how much data leaves the device, and to whom. No certified tier permits advertising identifiers or any connection to advertising-technology vendors. An app may be tested and shown without a tier — assessed, but not certified.

Validity and verification

Each app is re-assessed on every release, and its tier changes if its behaviour changes. This PDF is a snapshot of the release named above; the current, authoritative record is the app's page on stemp.li, where it can be checked against the certificate identifier shown.

Scope and limitations

The assessment covers the tested release and the behaviour observed during testing, described per release. A server's location does not by itself establish legal jurisdiction. This is a privacy assessment, not a regulatory, legal or medical approval.