

Riseform — Privacy Policy

Version: 1.0

Effective date: 17 September 2026

Last updated: 17 September 2026

Published at: <https://riseform.io/privacy>

0. Summary — the short version

Riseform is built so that your data stays with you.

- **Everything you record stays on your device.** Training logs, body measurements, protocol and cycle entries, laboratory results, notes and photographs are stored in a database on your iPhone.
- **We never receive your data.** We operate no servers for the App, no user accounts and no back end. There is no way for us to see, retrieve, restore or delete what you record.
- **No analytics, no advertising, no tracking.** The App contains no analytics tools, no advertising networks and no tracking technologies. We do not ask for permission to track you, because we do not track you.
- **Synchronisation is through your own iCloud.** If you enable it, your data is mirrored into the *private* database of *your* Apple Account, where Apple's own encryption and terms apply. We have no access to that database.
- **Apple Health data is used only in the App, on your device.** It is never used for advertising or marketing, never data-mined, and never shared with anyone.
- **The website riseform.io** is a static marketing page. It sets no cookies and runs no analytics. Its server keeps short-lived technical logs, and it currently loads a font file from Google — see Section 12.
- **The App is for adults (18+) only.**

The rest of this document sets out the detail required by the General Data Protection Regulation (Regulation (EU) 2016/679, “**GDPR**”) and by Apple's App Store requirements.

1. Who is responsible for your data

For processing for which we determine the purposes and means, the controller is:

Kanstantsin Vaitsakhouski

Individual developer

Józefa Sierakowskiego 3/8, 03-712, Warsaw, Poland

Privacy contact: privacy.riseform@kvdd.eu

We are not required to appoint a Data Protection Officer. Privacy enquiries go to the address above.

An important qualification. Because the App stores your data on your own device and, at your option, in your own iCloud account, and because we receive none of it, the great majority of the processing described in this policy is processing **you** carry out for your own purely personal purposes. Under Article 2(2)(c) GDPR, such processing falls outside the scope of the GDPR. We describe it in full anyway, so that you know exactly what the software does. Where the GDPR does apply to us — principally in respect of the Website and of correspondence you send us — we act as controller and this policy sets out the corresponding information under Articles 13 and 14 GDPR.

2. What this policy covers

This policy covers:

- the **Riseform** application for iPhone (the “**App**”);
- the **Riseform** companion application for Apple Watch;
- the **Riseform** Live Activity and widget;
- **Riseform GymDesk**, the optional companion application for macOS;
- the **website** at <https://riseform.io> (the “**Website**”).

It does not cover Apple’s own processing of your data as the operator of the App Store, iCloud, Apple Health and your Apple Account — that is governed by the **Apple Privacy Policy** (<https://www.apple.com/legal/privacy/>) — nor any third-party website you reach by following a link from the App.

3. The categories of data the App handles

All of the following is entered by you or read from your device with your permission, and all of it is stored **on your device**.

3.1 Training data

Training days, exercises (including any you create), sets, weights, repetitions, rest intervals, workout start and end times, duration, tonnage, personal records, workout history and the calendar of your activity.

3.2 Body metrics

Body weight, height, body-fat percentage, muscle percentage, and circumferences of the neck, shoulders, chest, waist, hips, arms (biceps and forearm, left and right) and legs (thigh and calf, left and right), together with body proportions, goals, and the dated history of every value.

3.3 Data from Apple Health (HealthKit) — optional

If you grant permission, the App **reads**: body mass, height, body-fat percentage, waist circumference, active energy burned, heart rate, resting heart rate, date of birth and

biological sex. It **writes**: completed workouts and their active energy, and body mass, height, body-fat percentage and waist circumference when you edit them in the App. On Apple Watch, the App reads heart rate during a workout and writes the workout.

The read data is used solely to prefill your measurements, to estimate calories burned and to compute a training-load figure, on your device. See Section 10 for the specific commitments that apply to this category.

3.4 Protocol and cycle log — health data (special category)

Courses you create; substances (“compounds”), their concentration, form and source; vials and batches; doses; syringe types; volumes; logged injections with date, time, the side of the body used (left or right), and tags describing how the injection went (including free-text tags you write yourself); notes; and photographs of packaging, vials or ampoules that you attach.

3.5 Laboratory analyses — health data (special category)

Records of tests you have taken or planned: date, title, selected test tags, rich-text notes, the associated course (if any), and up to five attached files per record (photographs or PDF documents of results, up to 5 MB each).

3.6 Supplements

Supplement plans, substances, doses, intake schedules, logged intakes and adherence.

3.7 Settings and preferences

Units of measurement, theme, app icon, language, rest-timer settings, notification settings, motivational-phrase settings, the biometric app-lock setting, calendar-mirroring and automatic-backup settings, and the pairing secret for local synchronisation with Riseform GymDesk.

3.8 What the App does not collect

The App does not collect or generate: an account, a username or a password; your email address; contacts; precise or coarse location; your device’s advertising identifier; a device fingerprint; browsing history; usage analytics; crash reports sent to us; or any identifier that could be used to track you across apps or websites.

4. Where your data is stored, and who can reach it

4.1 On your device

The primary store is a local database on your iPhone, inside the App’s sandbox, protected by iOS file-level encryption and by your device passcode. If you enable the biometric app lock, the App additionally requires Face ID, Touch ID or your device passcode before its content is shown. Attached photographs and documents are stored in the same protected container. **We have no access to any of it.**

4.2 In your own iCloud (optional)

If iCloud is enabled for the App, your database is mirrored into the **private database** of your own Apple Account through Apple's CloudKit service, so that your data survives reinstalling the App and follows your devices. This is the only routine network path out of the App.

- The destination is **your** iCloud account, not a server of ours. We operate no server for the App.
- We cannot read, browse, export or delete the contents of your private CloudKit database. Access is controlled by Apple and by your Apple Account credentials.
- Apple processes this data as the provider of iCloud, under the Apple Privacy Policy and the iCloud terms, which include Apple's encryption arrangements. Whether the data is protected by Standard Data Protection or by Advanced Data Protection depends on the setting **you** choose in your Apple Account.
- Apple delivers change notifications to your devices by silent push. These notifications signal that something changed; they do not send your records to us.
- You can turn iCloud off for the App at any time in the iOS Settings app, or delete the App's iCloud data there.

4.3 Backup snapshots in your iCloud Drive (optional)

If automatic backup is enabled, the App writes a dated snapshot file (.gymbak) into the App's own folder in **your** iCloud Drive, visible in the Files app under "Riseform", keeping the most recent 14 files. These are restore points under your control. You can open, copy, move or delete them yourself. We never see them.

4.4 Synchronization with Riseform GymDesk over your local network (optional)

If you use the macOS companion application, the two applications find each other on your local network using Bonjour and exchange exercise-library and analysis records over a **TLS-encrypted connection** whose key is derived from a six-digit code you type once on the Mac. The code itself is never transmitted; a wrong code simply fails the handshake. After pairing, each side stores a random device secret. **This traffic stays on your local network and never passes through us.**

4.5 Device calendar (optional)

If calendar mirroring is enabled, the App creates a dedicated device calendar named "GymApp" and writes your completed workouts and upcoming injection and analysis reminders into it, so that they appear in the Apple Calendar app. It writes only into that dedicated calendar and reads nothing else from your calendars. If your calendar is itself synchronised with an account (for example iCloud or Google), those events will be synchronised by that account under that provider's terms — please bear that in mind before enabling this feature for sensitive reminders. Turning the feature off deletes the dedicated calendar and its events.

4.6 Notifications

Reminders for rest timers, injections, supplements and planned analyses are **local notifications** scheduled by the App on your device. They are not sent through us or through any notification server of ours. Notification text may appear on your Lock Screen; you can control this in iOS Settings.

4.7 Exports and files you share

When you export your history to a spreadsheet, or share a backup file, the file is created on your device and handed to the iOS share sheet. **Where it goes next is entirely your choice** — for example iCloud Drive, another app, or a messaging service. Once it leaves the App we have no control over it, and the receiving service's own privacy policy applies.

4.8 Camera and photo library

If you attach a photograph of packaging, an ampoule or a laboratory result, the App accesses your camera or photo library only for the item you select. Images are stored inside the App's own store. Photographs may contain metadata (including, if your camera saves it, location) — the App neither reads nor uses that metadata, but it may be preserved inside the stored file.

5. Why the App processes this data, and on what legal basis

Purpose	Data	Legal basis (where the GDPR applies)
Maintaining your training log and showing progress	Sections 3.1, 3.2	Performance of the contract (Art. 6(1)(b)); processing carried out by you for personal purposes falls outside the GDPR under Art. 2(2)(c)
Reading and writing Apple Health data	Section 3.3	Your explicit consent, given through the iOS Health permission sheet (Art. 6(1)(a) and Art. 9(2)(a))
Maintaining the protocol, cycle and supplement log	Sections 3.4, 3.6	Your explicit consent, given by choosing to record this data (Art. 6(1)(a) and Art. 9(2)(a))
Maintaining the laboratory-analysis log and attachments	Section 3.5	Your explicit consent (Art. 6(1)(a) and Art. 9(2)(a))
Reminders and notifications	Sections 3.4–3.7	Your explicit consent, given by enabling notifications
Synchronisation to your iCloud and backup snapshots	All of Section 3	Your consent, given by enabling iCloud for the App (Art. 6(1)(a)); Apple processes as your iCloud provider
Local-network synchronisation with Riseform GymDesk	Exercise library, training days, analyses	Your consent, given by pairing the devices

Purpose	Data	Legal basis (where the GDPR applies)
Calendar mirroring	Workouts, upcoming reminders	Your explicit consent, given through the iOS Calendar permission sheet
App settings and lock	Section 3.7	Performance of the contract (Art. 6(1)(b))
Operating the Website	Section 12	Our legitimate interest in providing and securing the site (Art. 6(1)(f))
Answering your support or legal enquiry	The content of your message	Performance of the contract or our legitimate interest in responding (Art. 6(1)(b)/(f))

6. Special category (health) data

6.1. Body metrics, Apple Health data, protocol and cycle entries, supplement records and laboratory analyses are **data concerning health** within the meaning of Article 4(15) GDPR and are special category data under Article 9(1).

6.2. Where this data is processed under our responsibility, the legal basis is your **explicit consent** under Article 9(2)(a) GDPR. You give that consent by choosing to enable a feature and to record the data.

6.3. **You may withdraw consent at any time.** You do so by turning the relevant permission off (in the App, or in iOS Settings → Privacy & Security → Health / Calendars / Photos / Notifications), by disabling iCloud for the App, or by deleting the records or the App. Withdrawal does not affect the lawfulness of processing before withdrawal.

6.4. This data never leaves the paths described in Section 4. It is not transmitted to us, is not shared with any third party, is not used for advertising or marketing, and is not used to build any profile.

7. Automated decision-making and profiling

The App carries out **no** automated decision-making producing legal effects concerning you or similarly significantly affecting you, within the meaning of Article 22 GDPR, and **no** profiling. All “intelligent” behaviour — day rotation, weight prefill, calorie and training-load estimates, suggested laboratory-test checklists, injection-site observations, adherence figures — is produced by fixed arithmetic rules applied to your own entries, on your device. The App uses no machine learning and no artificial intelligence.

8. Who we share data with

We share your App data with no one, because we never have it.

There are no analytics providers, no advertising networks, no attribution or crash-reporting SDKs, and no third-party libraries that transmit data. The App contains no third-party software development kits at all.

The only parties that may be involved in processing, and only in the ways described above, are:

Party	Role	What is involved
Apple (Apple Inc. / Apple Distribution International Ltd., Ireland)	Provider of the platform, App Store, iCloud, Apple Health and push infrastructure, acting under its own privacy policy	Distribution of the App; your private CloudKit database; iCloud Drive backups; Apple Health; App Store purchase and billing data, which Apple collects directly from you and which we see only as aggregated, anonymised sales and performance statistics that do not identify you
Your calendar provider , if you enable calendar mirroring	Whichever account your device calendar syncs with, under its own terms	Workout and reminder events written into the dedicated calendar
Recipients you choose when exporting or sharing a file	Chosen by you, under their own terms	The exported file
DigitalOcean, LLC (Website hosting, Frankfurt, Germany)	Processor for the Website	Server access logs — see Section 12
Google Ireland Ltd. / Google LLC (web fonts on the Website)	Third party, under its own terms	Your IP address when a font is requested — see Section 12

We do not sell personal data, and we do not share personal data for cross-context behavioural advertising. We would disclose data only if we were compelled to do so by a valid legal obligation — and in respect of your App data we would have nothing to disclose.

9. Tracking and the App Tracking Transparency framework

The App does not track you. It does not access the advertising identifier, does not link your data with data from other companies for advertising or measurement, and does not share data with data brokers. For that reason, it does not present the App Tracking Transparency permission request. This is consistent with our App Store privacy declaration.

10. Specific commitments regarding Apple Health data

In accordance with Apple’s requirements for apps that use HealthKit, we confirm that:

- (a) the specific health data the App reads from and writes to Apple Health is disclosed in Section 3.3 of this policy;

- (b) health, fitness and medical data obtained through HealthKit is **never** used for advertising, marketing, use-based data mining or any purpose other than the health- and fitness-management functions of the App described here;
- (c) that data is **never** disclosed or sold to any third party;
- (d) the App does not write false or inaccurate data into Apple Health; and
- (e) the App is not used for, and does not conduct, health-related human-subject research.

11. The App is not a medical device

Riseform is a personal record-keeping and fitness tool. It is not intended for any medical purpose, is not a medical device under Regulation (EU) 2017/745, and provides no medical, diagnostic or dosing advice. See Section 9 of the **Terms of Use** for the full disclaimer.

12. The Website (riseform.io)

The Website is a static marketing page. It has no user accounts, no forms, no comment function and no newsletter.

12.1. No cookies, no analytics. The Website sets no cookies of its own and contains no analytics, advertising or tracking scripts. No consent banner is presented because no consent-requiring technology is used.

12.2. Server logs. The Website is served by nginx on a virtual server rented from **DigitalOcean, LLC** located in **Frankfurt, Germany**. Standard web-server access logs record your IP address, the date and time of the request, the resource requested, the HTTP status code, the volume of data transferred, the referring page and your browser's user-agent string. We use these logs solely to operate the site, to diagnose faults and to detect and defend against attacks. The legal basis is our legitimate interest in the secure and reliable operation of the site (Article 6(1)(f) GDPR). Logs are retained for no longer than **[30] days** and then deleted or rotated out.

12.3. Web fonts. The Website currently loads a typeface from **Google Fonts** (fonts.googleapis.com and fonts.gstatic.com). When your browser requests the font, your IP address and user-agent are transmitted to Google, which may process them outside the European Economic Area, including in the United States. Google relies on the European Commission's adequacy decision for the EU-US Data Privacy Framework and on standard contractual clauses. The legal basis for this transmission is our legitimate interest in a consistent visual presentation of the site (Article 6(1)(f) GDPR). *We intend to replace this with a self-hosted font so that no request leaves our own server; when we do, this section will be updated.*

12.4. Hosting provider as processor. DigitalOcean processes data on our behalf under a data processing agreement and the EU standard contractual clauses where applicable.

12.5. Links. The Website may link to the App Store and to other third-party sites. Once you follow such a link, the destination operator's privacy policy applies.

13. International transfers

13.1. Data in the App does not leave your device except by the paths in Section 4, all of which are within Apple's infrastructure or your own local network. Apple may store iCloud data in data centres in several countries; Apple's transfer safeguards are described in the Apple Privacy Policy.

13.2. For the Website, hosting is within the European Union (Frankfurt). The transmission to Google described in Section 12.3 may involve a transfer to the United States, safeguarded as described there.

13.3. We ourselves transfer no App data anywhere, because we hold none.

14. How long data is kept

Data	Retention
Everything you record in the App	Until you delete it — the individual record, the App's data, or the App itself. The App never silently deletes your data; a store it cannot read is quarantined rather than erased, so that recovery remains possible.
Data mirrored to your private iCloud database	Until you delete it, or delete the App's iCloud data in iOS Settings, or close your Apple Account. Governed by Apple's retention rules.
Automatic backup snapshots in your iCloud Drive	The most recent 14 daily files; older ones are deleted automatically. You may delete any of them yourself at any time.
Events in the dedicated device calendar	Until you disable calendar mirroring (which deletes the calendar) or delete them yourself.
Website server logs	Up to [30] days.
Support and legal correspondence	Up to 3 years from the last message, or longer where necessary to establish, exercise or defend legal claims, or to comply with a legal obligation.

15. Security

15.1. **On the device.** Your data is stored inside the App's sandbox and protected by iOS data protection and your device passcode or biometrics. The App offers an additional biometric lock (Face ID / Touch ID with passcode fallback) that hides its content when the App is not in the foreground.

15.2. **In transit.** iCloud synchronisation is encrypted by Apple. Local-network synchronisation with Riseform GymDesk uses TLS with a pre-shared key derived from a pairing code that is never transmitted. The Website is served over HTTPS.

15.3. **By design.** The strongest security measure in Riseform is architectural: there is no server, no account and no central database, so there is no central target to breach and no dataset of ours that could be exposed.

15.4. **Your part.** Please use a device passcode, keep iOS up to date, enable the in-app lock if your data is sensitive to you, consider enabling Apple's Advanced Data Protection for iCloud, and be careful where you send exported files.

15.5. **Breach notification.** No security measure is perfect. In the unlikely event of a personal data breach affecting data for which we are responsible, we will notify the competent supervisory authority and, where required by Article 34 GDPR, affected individuals.

16. Your rights

16.1. Where the GDPR applies, you have the right to: **access** your data (Art. 15); have it **rectified** (Art. 16); have it **erased** (Art. 17); **restrict** processing (Art. 18); receive it in a portable format (Art. 20); **object** to processing based on legitimate interests (Art. 21); and **withdraw consent** at any time (Art. 7(3)).

16.2. How the App's architecture affects this — and why it works in your favour.

Because your data never reaches us, we cannot answer an access or erasure request in respect of it: we have nothing to search and nothing to delete. Instead, you exercise these rights directly and immediately, without asking anyone:

- **Access and portability** — open any record in the App, and use **Export** to produce a spreadsheet of your entire history, or **Backup** to produce a complete machine-readable snapshot file.
- **Rectification** — edit or delete any record in the App.
- **Erasure** — delete individual records; delete all App data; disable and delete the App's iCloud data in iOS Settings → your name → iCloud; delete backup snapshots from the Files app; and delete the App from your devices.
- **Restriction and objection** — turn off the relevant feature or permission.
- **Withdrawal of consent** — revoke Health, Calendar, Photos, Camera, Local Network or Notification permission in iOS Settings; disable iCloud for the App; unpair Riseform GymDesk.

16.3. For data we do hold — correspondence you send us, and Website logs — write to **privacy.riseform@kvdd.eu**. We will respond within one month of receipt, extendable by two further months for complex requests, and will tell you if an extension is needed. We may need to ask for information to verify your identity. Exercising your rights is free of charge, unless a request is manifestly unfounded or excessive.

16.4. **Right to complain.** You may lodge a complaint with a supervisory authority, in the Member State of your habitual residence, place of work or of the alleged infringement. Our lead authority is:

Prezes Urzędu Ochrony Danych Osobowych (UODO)

ul. Stawki 2, 00-193 Warsaw, Poland

<https://uodo.gov.pl>

17. Children

17.1. The App is intended for **adults aged 18 and over** and is rated accordingly on the App Store. It is not directed at children, and we do not knowingly permit its use by anyone under 18.

17.2. We do not knowingly collect personal data from children. Because we collect no personal data from any user of the App, there is nothing for us to delete; if you believe a person under 18 is using the App, please contact us and, where you are their parent or guardian, remove the App from their device.

18. Consistency with our App Store privacy declaration

Our “App Privacy” declaration on the App Store product page states that **no data is collected from this app**. That declaration matches this policy: data recorded in the App remains on your device or in your own iCloud account and is neither transmitted to us nor collected by us.

19. Changes to this policy

19.1. We may update this policy to reflect changes to the App, to the Website, to our practices, or to the law.

19.2. The current version is always published at <https://riseform.io/privacy> with its version number and effective date. Where a change is material — in particular a change to the categories of data processed, the purposes, the recipients, or the legal bases — we will give notice in the App, on the Website or by other appropriate means before it takes effect, and, where the change relies on your consent, we will ask for your consent afresh.

19.3. Previous versions are available on request.

20. Contact

Kanstantsin Vaitsakhouski

Individual developer

Józefa Sierakowskiego 3/8, 03-712, Warsaw, Poland

Privacy contact: privacy.riseform@kvdd.eu

General and support: support.riseform@kvdd.eu

<https://riseform.io>

Riseform — Privacy Policy, version 1.0, effective 17 September 2026.