

FARO privacy policy

Last updated: 26 October 2026

This policy explains how we handle personal data in the FARO mobile apps for Android and iOS, in the FARO web app at app.farodive.com, in the FARO account those apps share, and on farodive.com. It is written for Regulation (EU) 2016/679 (GDPR) and for the Google Play user-data policy. The page you are reading is the privacy policy. [Download the same text as a PDF.](#)

Who we are

The controller is "SANTI" spółka z ograniczoną odpowiedzialnością, ul. Tadeusza Wendy 7/9, 81-341 Gdynia, Poland. KRS 0000157984. NIP 5882041600. REGON 192894764.

Santi makes diving equipment and publishes the FARO app. We have not appointed a data protection officer. Questions about this policy, and requests to use your rights, go to santi@santidiving.com or support@farodive.com. You can also call +48 58 678 50 10, or use the contact form on santidiving.com.

What this policy covers

It covers:

- the FARO app on Google Play and the App Store
- the FARO web app at app.farodive.com
- the FARO account, including dive logs and device data stored for that account
- farodive.com, including a request to order and the newsletter

Santi also processes personal data for its other products, dealers, service, and events. That processing is described at the end of this policy. It is separate from the FARO app.

Data we collect in the FARO app

We collect only what the app needs in order to run.

Account. Name, email address, and the sign-in method you choose: email and password, Google, Apple, or Facebook. Facebook is used only to sign in. We do not use the advertising identifier, and we do not turn on Facebook advertiser ID collection.

Profile photo. Optional. If you add one, you can take it with the camera or choose it from your photo library. We store the photo with your account.

Dive logs. When you download a log from your dive computer, the app receives the log the computer holds and stores it in your account so you can open it later. A log can include the dive time, depth profile, gas settings, and the other fields the computer recorded. We do not add a GPS track to the log.

Your equipment. Serial numbers and firmware versions of the dive computer and the docking station, the Bluetooth identity needed to reconnect, and configuration files you choose to send to the computer.

Bluetooth. The phone connects to the docking station, not directly to the computer. On Android 6 through 11 the operating system requires a location permission before an app can scan for Bluetooth devices. We use that permission only to find the station. We do not read, store, or share your GPS position. From Android 12 the scan is declared as never used for location.

Diagnostics. If the app crashes, Firebase Crashlytics receives a crash report: the error, the device model, the operating-system version, the app version, and a technical identifier of the selected device. We use this to fix faults. We do not use it for advertising.

We do not sell personal data. We do not show ads in the app. We do not make decisions about you that are based solely on automated processing and that produce legal effects, or similarly significant effects.

Data we collect on this website

If you send a request to order, we receive the name, email address, country, product, and any phone number or message you include. That form also has an optional box for product news. You can send the request without ticking it. If you join the newsletter and tick the consent box, we receive your email address and the fact that you agreed to hear from us. Neither box is pre-ticked. The honeypot field on the form is there to catch scripts. A person who fills it in is not stored as a subscriber.

The site does not run an advertising cookie or a third-party analytics cookie.

Why we use the data, and the legal basis

Purpose	Data	Legal basis
Create and run your FARO account, store dive logs, and sync a configuration you send	Account, logs, equipment, photo	Contract, GDPR Article 6(1)(b)
Connect the phone to your station	Bluetooth data, and the Android location permission described above	Contract, GDPR Article 6(1)(b)
Answer a request to order or a support message	Contact details and the message	Steps before a contract, or our legitimate interest in answering you, GDPR Article 6(1)(b) or 6(1)(f)
Send the newsletter	Email address and your consent	Consent, GDPR Article 6(1)(a). You can withdraw it at any time
Fix crashes and keep the service secure	Crash reports and security logs	Legitimate interest, GDPR Article 6(1)(f)
Keep invoices and tax records when a sale happens	Billing details	Legal obligation, GDPR Article 6(1)(c)
Defend or bring a legal claim	The records needed for that claim	Legitimate interest, GDPR Article 6(1)(f)

You do not have to create an account. Without one, the app cannot store logs in your name. You do not have to join the newsletter to use the app or to send a request.

Who receives data

People at Santi who operate FARO, and these processors, who act on our instructions:

- Google (Firebase Authentication, Cloud Firestore, Cloud Storage, Crashlytics, and Cloud Functions) hosts the account, logs, files, and crash reports
- Google, Apple, and Meta, only when you choose that provider to sign in
- Our email and hosting providers, for messages you send us and for this website

We also disclose data when the law requires it, for example to a tax authority or a court.

Transfers outside the European Economic Area

Santi is in Poland. Our processors include companies in the United States. Where a transfer is not already covered by an adequacy decision, we use the European Commission's Standard Contractual Clauses. Google LLC is certified under the EU-US Data Privacy Framework. You can ask us for a copy of the safeguards that apply to a transfer.

How long we keep data

- Account, dive logs, configurations, and the profile photo: for as long as the account exists. After a deletion request we remove them from active systems. Copies in backups are overwritten on the normal backup cycle and are not used for anything else.
- Crash reports: for up to 90 days.
- A request to order, and the related correspondence: for as long as we need to handle the request, and then for the period in which a claim about it can still be brought.
- Newsletter address: until you withdraw consent, and then only as a suppression record so we do not email you again.
- Invoices and tax records: for the period Polish accounting law requires, which is generally five years.

How we protect data

Traffic between the app and our servers uses TLS. Access to the account database is limited to the signed-in user and to the staff and services that operate FARO. The marketing site does not let a browser read the database directly. No method of transmission or storage is perfectly secure.

Your rights

You can ask us to:

- confirm whether we process your data, and for a copy of it
- correct data that is wrong
- delete data, or restrict what we do with it
- receive data you provided, in a portable format, where the basis is a contract or consent
- object to processing that is based on legitimate interest
- withdraw consent, where the basis is consent. Withdrawal does not affect processing that took place before it

We respond within one month. We may ask you to prove that you control the account, so that we do not hand data to someone else. To use any of these rights, email santi@santidiving.com or support@farodive.com.

You can also complain to a supervisory authority. In Poland that is the President of the Personal Data Protection Office (Prezes Urzędu Ochrony Danych Osobowych), ul. Stawki 2, 00-193 Warsaw, uodo.gov.pl. If you live in another EU or EEA country, you can complain to the authority of the country where you live, where you work, or where the issue happened.

Delete your FARO account

In the web app at app.farodive.com you can delete the sign-in from your profile. That removes the login. It does not, by itself, remove the dive logs, device records, or profile photo stored for the account.

To delete those as well, email support@farodive.com from the address on the account. Use the subject "Delete my FARO account" and tell us the email address of the account. We will delete the sign-in, the dive logs stored in it, device records linked to it, and the profile photo. We will keep a record only where the law requires it, such as an invoice. You can make the same request to santi@santidiving.com. You do not need the app installed to make this request.

Children

FARO is not directed at children under 16, and we do not knowingly create accounts for them. If you believe a child has given us personal data, email us and we will delete it.

Other processing by Santi

Outside the FARO app, Santi still processes personal data for the purposes in its earlier notice. The bases are the same ones named above: a contract, a legal duty, or a legitimate interest, and consent where we send optional marketing.

- answering questions by email, phone, a web form, or social media
- running the dealer and distributor network
- buying goods and services from suppliers
- accounting and tax records
- online sales of the afterdive collection
- warranty and post-warranty service of equipment
- the Stay Dry Club, for clients who choose that programme
- the Santi Photo/Video Awards, including photographs entrants send in
- keeping records the law requires us to archive
- debt collection and defence against claims

That data may be handled by IT, marketing, legal, and logistics providers, and by public authorities when the law requires it. The rights in this policy apply to that processing as well.

Contact santi@santidiving.com.

Changes

If we change this policy, we will update the date at the top and publish the new text at this address. Where the law requires it, we will also tell account holders in the app or by email.

Contact

"SANTI" spółka z ograniczoną odpowiedzialnością, ul. Tadeusza Wendy 7/9, 81-341 Gdynia, Poland. santi@santidiving.com. support@farodive.com. +48 58 678 50 10.