

# AgroCares Privacy Statement

Version 2.0 — Last updated: 30 April 2026

*This Statement supersedes the AgroCares Privacy Policy version 1 of 01 August 2023.*

This Statement explains how AgroCares uses your personal data when you use our products and services — the AgroCares Scanner Solutions app, Carbon Monitor (SoilCASTOR), Lab-in-a-Box, the AgroCares Portal, NutriOpt On-Site Adviser, MOBES, LabApp, our laboratory analytical services, and our webshop — and when you contact us directly.

## Who we are

We are **Care4Agro B.V.**, trading as **AgroCares**, a Dutch company registered with the Chamber of Commerce under number **76517721** (VAT NL860654709B01). Our registered office is at **Nieuwe Kanaal 7C, 6709 PA Wageningen, Netherlands**, and our laboratory is at **Nieuwe Kanaal 7, Wageningen**. We are the controller of the personal data described below, except where we expressly act as a processor for one of our partners (see “When we are a processor for someone else”).

## Contact

If you have questions about this Statement, want to exercise your rights, or want to make a complaint, please contact us:

- Email: [info@agrocared.com](mailto:info@agrocared.com)
- Subject line: “Privacy request”
- Postal: Care4Agro B.V., Nieuwe Kanaal 7C, 6709 PA Wageningen, Netherlands

We will respond within one month of receiving your request, and may extend this by up to two further months for complex requests, in which case we will tell you within the first month.

## What personal data we use

We use only the personal data we need to deliver our products and services. The categories of data we use are:

- **Identity and contact data** — your name, email address, phone number, the organisation you work for, your role.
- **Account data** — your username, password (stored in hashed form, never in plain text), preferences, login timestamps, IP address, language preference.
- **Field and scan data** — when you take a scan, we collect the GPS coordinates of the sample location, the device serial number, and a timestamp. The spectral data and

analytical results themselves are not personal data on their own, but we treat them as personal data when they are linked to your account.

- **Laboratory sample data** — when you submit a sample to our Laboratory, we record your contact and shipping details and a unique sample identification number that links your sample to your customer record.
- **Support data** — the content of any support enquiry you make, including any information you choose to include.
- **Order and billing data** — billing address, shipping address, email, phone, order history, invoices. We do **not** store your payment-card data; that is handled by the payment provider directly.
- **Marketing data** — your preferences for marketing communications and your engagement with our messages.
- **Website and app usage data** — when you use our website or mobile applications and have accepted analytics cookies/consent, we collect a truncated IP address, device identifier, browser/OS version, page-view metrics, and crash logs (mobile only). This data does not include your name or email address.

We do not collect special categories of personal data (such as data concerning health, ethnicity, or political opinions), and we do not knowingly collect personal data from children.

### Why we use your personal data and on what legal basis

What we do	Why	Legal basis
Operate your AgroCares account, deliver the analytical services you have purchased, return your results and reports	To perform the contract you have entered into with us	Article 6(1)(b) GDPR — contract performance
Generate carbon-sequestration projections in Carbon Monitor	To perform the contract	Article 6(1)(b)
Operate NutriOpt On-Site Adviser on behalf of Nutreco (where you are a Nutreco customer)	To perform our partnership contract; we act as processor for Nutreco	Article 6(1)(b)
Operate MOBES on behalf of HLB (where you are an HLB customer or scout)	To perform our partnership contract; we act as processor for HLB	Article 6(1)(b)
Process samples received at our Laboratory and return analytical results	To perform the contract for the analytical service	Article 6(1)(b)
Respond to your support enquiries	To perform the contract	Article 6(1)(b)
Process your webshop order, take payment via our payment	Contract performance and complying with our fiscal-record	Articles 6(1)(b) and 6(1)(c)

What we do	Why	Legal basis
provider, ship your order, and keep records	obligations	
Send you marketing communications	If you are an existing customer, our legitimate interest in marketing similar products to you (you can object at any time); otherwise, your consent	Articles 6(1)(f) and 6(1)(a)
Improve our calibration models on a fully aggregated, anonymised basis	Our legitimate interest in improving service quality	Article 6(1)(f)
Measure how visitors use our website and mobile apps	Where we use Google Analytics or Firebase for analytics, we ask for your consent through the cookie banner and in-app prompt	Article 6(1)(a) — consent

### How long we keep your personal data

- **Account data:** for as long as your account is active. After you close your account, we delete or anonymise your personal data within 90 days, except where we are legally required to retain it longer (for example, fiscal records).
- **Scan data and analytical results:** retained for the lifetime of your account so that your historical reports continue to be available. On account closure or on your erasure request, the link between scans and your identity is removed.
- **Physical samples submitted to our Laboratory:** retained for **30 days** after your results are reported, then destroyed (or returned to you at your cost on written request).
- **Order and billing data:** retained for **7 years** as required by Dutch fiscal law.
- **Support data:** retained for **3 years** after the close of your support ticket.
- **Marketing data:** retained until you withdraw consent or object; engagement metrics are retained on a 2-year rolling basis.
- **Website and app analytics data:** Google Analytics retention is set to 14 months; Firebase Crashlytics 90 days; Firebase Analytics 14 months.
- **Backups:** automatic backups age out within 30 days of the weekly-full backup retention window.

### Who we share your personal data with

We share your personal data only with the following categories of recipient, and only to the extent needed to deliver the relevant service or comply with the law:

- **Cloud-infrastructure provider** — provides the cloud platform and productivity services we use to host your data. All AgroCares production data is stored in the European Union (West Europe region, Netherlands).

- **Our group's development team** — a related entity within our corporate group, located in Türkiye, whose personnel form our development team and process data on our instructions when developing, deploying, and operating our services.
- **Our cloud solution provider partner** — located in Türkiye, handles cloud subscription billing, licensing, and tenant-administration operations.
- **Our partner controllers (Nutreco, HLB, NMI)** — where you are a customer or user of one of our partner services (NutriOpt On-Site Adviser, MOBES, grasplan, or the NMI Portal), your data is processed on the partner's instructions and shared back with that partner as the controller of that service.
- **Payment-gateway provider** — established in the Netherlands; handles your payment-card data on our behalf when you make a webshop purchase.
- **HR and payroll providers** — established in the European Economic Area; provide our HR and payroll systems for staff and contractor data.
- **Other SaaS providers** — providers of our project-management, customer-support, source-control, email-delivery, and website-security tooling.
- **Analytics provider** — provides website and mobile-app analytics services. Configured with EU data-residency settings and IP truncation.

We do not sell your personal data. We do not share your personal data with anyone for their own marketing purposes. **We do not share your personal or financial data with credit reference agencies, banks, or credit insurers.**

A current list of the specific service providers we engage in each of the above categories is maintained internally and is available on request to data subjects, supervisory authorities, and partners with a legitimate interest, subject to our reasonable confidentiality requirements.

## Transfers outside the European Economic Area

Most of your personal data stays inside the European Economic Area. Where it does leave the EEA, we use the European Commission's Standard Contractual Clauses (with any supplementary measures required) to ensure that your data continues to receive an adequate level of protection. Specifically:

- **Türkiye** — our group development team and our cloud solution provider partner have access to our systems for development, operations, and tenant administration. We have entered into Standard Contractual Clauses with each and apply supplementary technical and organisational safeguards.
- **United States** — certain SaaS providers we engage (for customer support, source control, email delivery, analytics, and website security) are based in or operate from the United States. Each operates under Standard Contractual Clauses incorporated in their data-processing agreements with us, with supplementary measures including EU data-residency configurations where the provider supports them.
- **Partner Controller — Nutreco group (NutriOpt customers only)** — Nutreco operates internationally. Where you are a Nutreco customer, your data may be

accessed by Nutreco entities outside the EEA under the Data Processing Agreement we have with Nutreco, which incorporates the Standard Contractual Clauses.

## When we are a processor for someone else

For specific products we act as a processor under GDPR Article 28, not as the controller:

- **NutriOpt On-Site Adviser** — Nutreco Nederland B.V. is the controller; we operate the platform on their behalf.
- **MOBES** — HLB is the controller; we operate the platform on their behalf.
- **grasp1an and the NMI Portal** — NMI is the controller; we operate the platform on their behalf.

For these products, the relevant partner's privacy notice applies in addition to ours, and we follow their instructions regarding your data.

## Your rights

Under the GDPR, you have the following rights in respect of your personal data:

- **Access** (Article 15) — to obtain a copy of the personal data we hold about you.
- **Rectification** (Article 16) — to correct inaccurate or incomplete data.
- **Erasure** (Article 17) — to have your data deleted, subject to legal retention obligations.
- **Restriction** (Article 18) — to limit how we use your data while we resolve a question.
- **Data portability** (Article 20) — to receive your data in a structured, machine-readable format and have it transmitted to another controller.
- **Objection** (Article 21) — to object to processing based on our legitimate interest, including objection to direct marketing.
- **Withdraw consent** — where we rely on your consent, you can withdraw it at any time without affecting the lawfulness of processing carried out before withdrawal.
- **Not be subject to automated decision-making** (Article 22) — we do not make solely automated decisions that produce legal effects concerning you.

You can exercise these rights through your account settings (where supported) or by contacting [info@agrocared.com](mailto:info@agrocared.com).

## Right to complain

If you believe our processing of your personal data infringes the GDPR, you have the right to lodge a complaint with a supervisory authority — in the Netherlands, the Autoriteit Persoonsgegevens ([autoriteitpersoonsgegevens.nl](http://autoriteitpersoonsgegevens.nl)). We would appreciate the opportunity to address your concern first.

## How we keep your personal data secure

We protect your personal data with appropriate technical and organisational measures, including encryption in transit (TLS 1.2 or higher) and encryption at rest, role-based access control, multi-factor authentication for our staff, continuous vulnerability monitoring, regular backups, and a documented incident-response process. Our Information Security Policy is reviewed annually.

## Cookies, similar technologies, and analytics

When you use the AgroCares Portal, our webshop, or our website, we use cookies and similar technologies to operate the service, remember your preferences, and — with your consent — measure how the service is used.

Specifically:

- **Essential cookies** — required to make the site work (login session, shopping cart, security). These do not require your consent.
- **Analytics — Google Analytics 4** — when you accept analytics cookies, we use Google Analytics to understand how visitors use the website. The data sent to Google is configured for EU data residency and IP-address truncation to limit what is identifiable. Retention is set to 14 months.
- **Mobile-app analytics — Firebase** — our mobile applications use Firebase (a Google service) for usage analytics, crash reporting, and push notifications. You can turn this off in the app settings.

You can manage your cookie preferences through the cookie banner on first visit and at any time afterwards through the cookie-settings link in the footer.

## Changes to this Statement

We may update this Statement from time to time. The “Last updated” date at the top reflects the most recent revision. Where the changes are material, we will let you know in advance — for example, by email or by a notice in the application — so that you have the opportunity to review them before they take effect.