Privacy and Cookies Policy

Sunrise Poultry Farms Ltd

Last updated and effective date: 25.11.2026.

Publication checks: yellow highlighted items and the verification schedule at the end must be resolved before publication.

1 Introduction and scope

Sunrise Poultry Farms Ltd (Sunrise, we, us or our) is committed to protecting personal data and respecting your privacy. This policy explains how we collect, use, retain, share and protect personal data, and how you can exercise your rights.

It applies to visitors to our website, prospective, current and former customers and suppliers, their representatives, and other individuals who contact or conduct business with us. Personal data means information relating to an identified or identifiable living person (it includes business contact details that identify an individual).

Recruitment, employment and worker information is covered by separate privacy notices. This policy does not describe our recruitment or employee processing. Specific notices for other activities, such as site visits or CCTV where applicable, should be read alongside this policy.

We process personal data in accordance with the United Kingdom General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), each as amended, including by applicable provisions of the Data (Use and Access) Act 2025.

2 Who we are and how to contact us

Sunrise Poultry Farms Ltd is the controller when it determines why and how your personal data is processed.

Registered legal name: Sunrise Poultry Farms Limited
Company registration number: 01135442
Registered office and postal contact: 250 Seagrave Road, Sileby, Loughborough, England, LE12 7NJ
Email: info@sunrise-eggs.com
Telephone: 01509 812441

Sunrise forms part of the AGROVA group. Other group companies may support relevant corporate, administrative, financial, IT and compliance functions. Sharing is subject to the requirements in sections 9 and 10. If another entity acts as a separate or joint controller, we will provide the relevant controller information as required by law.

3 The personal data we collect

The information we process depends on your relationship with us. We collect only information that is adequate, relevant and limited to what is necessary for the purpose concerned.

Identity and contact data

Your name, job title, employer or business name, business or delivery address, email address and telephone number.

Commercial and transaction data

Customer and supplier records, contractual arrangements, orders, deliveries, invoices, payment records and relevant commercial correspondence.

Financial data

Bank account or payment details where necessary to make or receive payments. This does not imply that we collect payment card details.

Communications data

Information you provide in enquiries, feedback, complaints, emails and other correspondence. Reference to telephone communications does not mean that calls are recorded.

Technical and usage data

Where generated by the website or its services: IP address, browser and device information, cookie identifiers, pages visited and website interactions.

Marketing preferences

Your communication preferences, consent records where relevant, and records of objections or opt-outs.

Visitor and security data

When you visit our production facilities, we may collect your name, organisation, contact details, purpose of visit, arrival and departure times, and other information necessary to manage site access, security, health and safety and biosecurity requirements.

For visits to poultry production facilities, we may also collect information about recent contact with poultry or other animals and other circumstances relevant to biosecurity. Where applicable, CCTV images may be collected for security and safety purposes.

Where additional personal data, including health-related information, is required, we will process it in accordance with applicable data protection law and provide further privacy information where necessary.

4 How we obtain personal data

Where we obtain personal data from sources other than directly from you, we will provide the information required by applicable data protection law within the relevant timeframe, unless an exemption applies.

5 Purposes and lawful bases

The table links the principal purposes to the data involved and the relevant lawful basis. We use a basis only where its conditions are met. Contract applies where you personally are a party to the contract, or ask us to take steps before entering one (processing the details of an employee of a corporate customer or supplier will usually rely on legitimate interests instead).

Purpose	Personal data	Lawful basis and relevant interest
Responding to enquiries and managing business relationships	Identity, contact and communications	Legitimate interests in responding to contacts and maintaining business relationships. Contract for steps requested by an individual before a contract, where applicable.
Managing customer orders, deliveries and payments	Identity, contact, commercial, transaction and financial	Contract with an individual customer. Otherwise, legitimate interests in supplying products, administering orders and receiving payment. Legal obligation for applicable accounting and tax records.
Managing suppliers and paying invoices	Identity, contact, commercial, transaction and financial	Contract with an individual supplier. Otherwise, legitimate interests in procuring goods and services and paying suppliers. Legal obligation for applicable accounting and tax records.

Purpose	Personal data	Lawful basis and relevant interest
Handling feedback, complaints and product issues	Identity, contact, communications and relevant transaction details	Legitimate interests in investigating concerns, improving products and resolving disputes. Legal obligation where a specific product safety or regulatory duty applies. Any health data requires a separate Article 9 condition.
Business administration	Relevant business contact, commercial, transaction and communications data	Legitimate interests in proportionate group reporting, IT support, administration, audit and risk management. Legal obligation where specific statutory reporting duties apply.
Securing the website and information systems	Technical, usage and relevant identity and contact data	Legitimate interests in maintaining secure and reliable services and preventing fraud or misuse. Legal obligation where a specific data security duty applies.
Website analytics and optional functions where used	Technical, usage, cookie identifiers and preferences	Consent where required for device storage or access and associated personal data processing. Any PECR exception and separate UK GDPR basis must be verified before reliance on it (see section 8).
Sending permitted direct marketing	Identity, contact and marketing preferences	Consent where required. Otherwise legitimate interests in promoting our products and maintaining business relationships, subject to PECR and your right to object.
Site access and security where applicable	Visitor identity, contact, access records and CCTV images	Legitimate interests in protecting people, premises and property. Legal obligation where a specific safety duty applies. Details must match the local visitor or CCTV notice.
Legal claims, compliance, insurance and risk management	Relevant identity, contact, communications, transaction and financial data	Legitimate interests in obtaining advice and insurance, preventing fraud and establishing or defending legal rights. Legal obligation where disclosure or retention is required by law.

6 How we apply lawful bases

Where we rely on legitimate interests, we consider whether the processing is necessary and balance our interests against your rights and freedoms.

Where we rely on consent, you may withdraw it at any time. This will not affect processing carried out lawfully before withdrawal.

If we intend to use personal data for a different purpose, we will ensure that the new use is permitted by law and provide additional information or obtain consent where required.

7 Direct marketing

We may occasionally contact our business customers and contacts with information about our products, services and relevant business developments, where permitted by applicable data protection and electronic marketing laws.

Where consent is required, we will obtain it before sending marketing communications.

You may object to receiving direct marketing communications at any time by contacting us at info@sunrise-eggs.com or using an unsubscribe option where provided.

8 Cookies and similar technologies

Our website may use cookies and similar technologies to support its operation, maintain security and improve the user experience. Cookies are small text files stored on your device when you visit a website. Some cookies are necessary for the website to function properly, while others may be used to understand how visitors interact with the website.

Where cookies or similar technologies require consent under applicable law, we will request your consent before using them. You may refuse or withdraw your consent at any time through the cookie preference controls provided on our website.

You can also manage or delete cookies through your browser settings. Please note that disabling certain cookies may affect website functionality.

Information about the cookies used on our website, including their purposes and duration, will be made available through our cookie information or preference settings.

9 Sharing personal data

We disclose personal data only where necessary and proportionate for an identified purpose, with an appropriate lawful basis and safeguards. Recipients may include the following, depending on the activity:

- AGROVA group companies providing relevant financial reporting, administration, IT, compliance, audit or risk management support. Common group ownership does not itself justify disclosure.
- Service providers supporting IT, cloud hosting, website operation, communications, payments, deliveries, security and other relevant business functions.
- Professional advisers, including lawyers, accountants, auditors and insurance advisers, financial institutions and insurers where relevant.
- HM Revenue & Customs, courts, law enforcement and other public authorities or regulators where disclosure is required or otherwise lawfully justified.

Where a provider processes personal data on our behalf, we require an appropriate Article 28 UK GDPR contract. Other recipients may be independent controllers, with their own legal responsibilities. Joint controller arrangements, where applicable, must allocate responsibilities transparently and make the essence of the arrangement available to you.

10 International transfers

As part of the AGROVA group, personal data may be shared with or accessed by authorised group companies and service providers located outside the United Kingdom, including in Latvia and other European Economic Area countries, where necessary for legitimate business purposes.

Where personal data is transferred internationally, we ensure that the transfer complies with applicable UK data protection legislation. This includes relying on applicable UK adequacy regulations or implementing appropriate safeguards where required.

You may contact us for further information about the safeguards applicable to international transfers of your personal data.

11 Data security

We use appropriate technical and organisational measures designed to protect personal data against unauthorised or unlawful processing and accidental loss, destruction, alteration or disclosure. Measures are selected according to the risks and may include access restrictions, authentication, secure storage and transmission, backup and recovery arrangements, staff confidentiality requirements, supplier controls and breach response procedures.

Access is limited to authorised people who need the information for their duties. If a personal data breach occurs, we assess it and notify the supervisory authority and affected individuals where the law requires. No method of internet transmission or storage can be guaranteed completely secure.

12 How long we retain personal data

We keep personal data only for as long as needed for its purpose and applicable legal, accounting, tax, regulatory and contractual requirements. The criteria below apply where a single fixed period cannot be given. Different records may need different periods.

- Customer and supplier records: the duration of the relationship and the period needed for transaction administration, statutory record keeping and relevant claims or audit requirements.
- Enquiries, correspondence and complaints: the time needed to resolve the matter, follow up and address any relevant claims, safety or regulatory requirements.
- Website and technical data: We retain technical and website usage information only for as long as necessary for the relevant operational, security or analytical purpose, subject to applicable legal requirements.
- Marketing communications: We retain contact details for as long as necessary for permitted marketing activities. Where someone objects to receiving marketing communications, we may retain limited information to ensure their preference is respected.
- Visitor and CCTV records, if used: a proportionate security period stated in the applicable notice, with relevant material retained longer only where needed for an incident, investigation or legal requirement.

We may preserve relevant records for an actual or reasonably anticipated dispute, investigation or legal hold. When data is no longer needed, we securely delete or anonymise it or otherwise dispose of it securely, including through appropriate backup expiry arrangements.

13 Your rights and how to use them

You may exercise your rights by contacting us using the details in Section 2. We may request information reasonably necessary to verify your identity or clarify your request.

We will respond without undue delay and within the timeframe required by applicable law, normally within one month. Where the law permits an extension or other adjustment, we will inform you as required.

Requests are generally free of charge. In limited circumstances permitted by law, we may charge a reasonable fee or refuse to act on a request, and we will explain the reasons for doing so.

14 Automated decision making

Sunrise does not use solely automated decision-making, including profiling, to make decisions that produce legal or similarly significant effects on individuals.

15 Other websites and changes to this policy

Our website may link to independently operated websites. Please read their privacy information before submitting personal data. Their operators are responsible for their own processing (this does not remove Sunrise' s responsibility for any disclosure or tracking it initiates).

We may update this policy to reflect changes in law, guidance or our processing. We publish the current version with its effective or last-updated date and provide additional notification of material changes where required.