Customer Privacy Notice

How Agricultural Central Trading Limited collects, uses, shares and protects personal data.

Effective 11 August 2026	Version 2

This notice applies to customers, prospective customers, account applicants, guarantors and other individuals whose personal data we process in connection with customer accounts, orders, credit facilities and related services. It explains what information we collect, where it comes from, why we use it and the rights available to you.

1. Who we are

Agricultural Central Trading Limited (ACT) is the data controller for the personal data covered by this notice. This means that ACT decides how and why that information is processed.

Legal entity	Agricultural Central Trading Limited
Registered office	Grange Court, Sitka Drive, Shrewsbury Business Park, Shropshire, SY2 6LG
Company number	00713606
ICO registration	Z5267857
Data Protection Officer	Glenn Foster gdpr@actionfarm.co.uk 01743 762700

2. Personal data we collect

We may collect and process the following categories of personal data where relevant:

- **Identity data** - name, title, date of birth and other information used to identify you.
- **Contact data** - postal address, email address and telephone number.
- **Account and application data** - account details, credit applications, account contacts, permissions and records relating to the opening and administration of an account.
- **Financial and transactional data** - payment and billing information, bank or payment details where required, purchase history, invoices, balances and transaction records.
- **Credit, affordability and risk data** - credit commitments, payment history, credit scores or indicators, identity verification results, fraud indicators and relevant public record information.
- **Communications data** - correspondence, emails, enquiries, complaints and records of our interactions with you.
- **Technical, security and audit data** - IP address, device or browser information, access records, system logs and incident-related information where you use our systems or online services.

- **Compliance data** - information required for legal, regulatory, accounting, audit, due diligence or fraud-prevention purposes.

3. Where personal data comes from

We may obtain personal data about you from:

- you directly, including through account applications, orders, correspondence and telephone or online contact;
- your employer, business, account holder, authorised representative, guarantor or other person connected with an application or account;
- credit reference agencies, including information obtained through Creditsafe and its data partner TransUnion;
- fraud-prevention, identity-verification, payment and other service providers;
- publicly available sources, including Companies House, court records, insolvency records, business websites and other public registers; and
- professional advisers, regulators, public authorities or other third parties where permitted by law.

4. Why we use personal data

We process personal data only where necessary and for defined, lawful purposes. These include:

- assessing and administering account and credit applications;
- supplying goods and services, processing orders, managing accounts, taking payment and fulfilling contractual obligations;
- managing customer, supplier and business relationships and responding to enquiries or complaints;
- assessing creditworthiness and affordability, verifying identity, preventing fraud, managing risk and recovering debts;
- complying with legal, regulatory, tax, accounting and contractual obligations;
- protecting the confidentiality, integrity and availability of personal data and our systems;
- managing system access, authentication, logging, monitoring and audit activities;
- detecting, preventing and responding to security incidents, unauthorised access or personal data breaches;
- maintaining records for governance, compliance, accountability and the establishment, exercise or defence of legal claims; and
- providing information about ACT products and services where permitted by law. You can opt out of direct marketing at any time.

5. Our lawful bases

We process personal data in accordance with the UK GDPR and the Data Protection Act 2018. Depending on the activity, we rely on one or more of the following lawful bases:

Performance of a contract

Processing is necessary to take steps at your request before entering into a contract or to perform our contractual obligations, including opening and managing accounts, processing orders and supplying goods or services.

Legal obligation

Processing is required to comply with applicable laws, regulatory requirements, accounting rules, tax obligations or other statutory duties.

Legitimate interests

Processing is necessary for ACT's legitimate business interests or those of a third party, provided those interests are not overridden by your rights and freedoms. Our legitimate interests include operating our business, assessing and managing credit risk, preventing fraud, protecting customers and ACT, maintaining system and data security, recovering debts, supporting audit and compliance, protecting TransUnion data and establishing or defending legal claims. We carry out appropriate assessments where required.

Consent

Where consent is required by law, you will be given a clear choice. You may withdraw consent at any time without affecting the lawfulness of processing carried out before withdrawal.

6. Credit reference and affordability checks

To help us assess applications, prevent fraud, and meet our legal and regulatory obligations, we may obtain information about you from credit reference agencies (CRAs).

We obtain this information via Creditsafe, which uses its data partner TransUnion to supply consumer credit and identity data.

Creditsafe Business Solutions Limited	Authorised and regulated by the Financial Conduct Authority FCA Firm Reference Number: 742313
TransUnion International UK Limited	Authorised and regulated by the Financial Conduct Authority FCA Firm Reference Number: 737740

The information we receive may include data relating to your identity, credit commitments, payment history, and public record information. This data is used solely for legitimate business purposes, including creditworthiness assessment, identity verification, affordability assessment and fraud prevention, in accordance with applicable data protection laws.

Further information about how Creditsafe and TransUnion process personal data is available in their privacy notices:

- Creditsafe Customer and Supplier Transparency Notice
- TransUnion Credit Reference Agency Information Notice (CRAIN)
- TransUnion Bureau Privacy Notice

7. Who we share personal data with

We share personal data only where there is a lawful reason and only to the extent necessary. Recipients may include:

- ACT employees, officers, agents and authorised contractors who need the information to perform their duties;
- Creditsafe, TransUnion and other credit-reference, identity-verification or fraud-prevention providers;

- service providers supporting IT, hosting, communications, payment processing, delivery, account administration and business operations;
- insurers, auditors, accountants, solicitors, debt-recovery providers and other professional advisers;
- banks, payment providers, business partners and suppliers where necessary to provide goods or services; and
- regulators, courts, law-enforcement bodies, tax authorities and other public bodies where disclosure is required or permitted by law.

We do not sell personal data and do not share it with third parties for their own unrelated marketing purposes.

8. International transfers

Some suppliers or recipients may process personal data outside the UK and/or the European Economic Area. Where this happens, we use appropriate safeguards required by data protection law. These may include a UK adequacy regulation, the UK International Data Transfer Agreement, the UK Addendum to approved standard contractual clauses, or another lawful transfer mechanism. You may contact us for more information about the safeguards relevant to your personal data.

9. How long we keep personal data

We keep personal data only for as long as necessary for the purpose for which it was collected and to meet legal, regulatory, accounting, tax, contractual or reporting obligations. When deciding how long to keep information, we consider:

- the nature, amount and sensitivity of the personal data;
- the purposes for which it is used and whether those purposes can be achieved in another way;
- the duration of the customer or business relationship and any applicable limitation periods;
- legal, regulatory, tax, audit and contractual requirements; and
- the need to prevent fraud, resolve disputes, recover debts or establish, exercise or defend legal claims.

Personal data used for credit-reference or affordability checks is retained only for as long as required for those purposes and is then securely deleted or anonymised. When personal data is no longer required, it is securely deleted, anonymised or otherwise disposed of in accordance with our retention arrangements.

10. Providing personal data

The provision of certain personal data is primarily contractual and, in some circumstances, is required to meet legal or regulatory obligations. Personal data may be needed to:

- enter into and perform a contract with you or the business you represent;
- process orders, manage accounts, take payment and supply goods or services;
- verify identity, assess creditworthiness or affordability and prevent fraud; and
- comply with legal, regulatory, accounting and tax obligations.

If you do not provide requested personal data, we may be unable to open an account, enter into a contract, fulfil an order, provide goods or services, or complete necessary verification, compliance or fraud-prevention checks. Services may therefore be delayed, restricted or declined.

Where personal data is requested for an optional purpose, such as certain marketing communications, providing it is not mandatory and you may withdraw consent or opt out at any time without affecting your ability to receive goods or services from us.

11. Automated tools and human review

We may use automated systems and tools to support risk assessment, fraud prevention, affordability checks, identity verification and record management. These tools may analyse personal data using predefined criteria or rules to generate indicators, scores or recommendations.

ACT does not make decisions that have a legal or similarly significant effect on an individual based solely on automated processing. Any such decision is subject to meaningful human review. Automated tools may influence the speed or level of review applied to an application, but an individual will not be automatically rejected or subjected to an adverse decision without human involvement.

If you have questions about a decision or believe it has been made solely by automated means, contact us using the details in section 1.

12. How we protect personal data

We use appropriate technical and organisational measures designed to protect personal data against accidental or unlawful loss, alteration, disclosure, access or destruction. Measures include access controls, authentication, staff responsibilities, system monitoring, secure storage, supplier controls, incident response arrangements and regular review of security measures. Access is limited to people who need the information for authorised purposes.

13. Your data protection rights

Depending on the circumstances and lawful basis, you may have the following rights:

- **Access** - request a copy of the personal data we hold about you and information about how it is used.
- **Rectification** - ask us to correct inaccurate or incomplete personal data.
- **Erasure** - ask us to delete personal data where there is no lawful reason for us to continue processing it.
- **Restriction** - ask us to limit how we use personal data in certain circumstances.
- **Data portability** - receive certain personal data in a structured, commonly used and machine-readable format and ask us to transfer it to another organisation where the right applies and this is technically feasible.
- **Object** - object to processing based on legitimate interests and object at any time to direct marketing.
- **Withdraw consent** - withdraw consent at any time where consent is the lawful basis for processing.

Your right to object	You have the right to object to processing based on legitimate interests. You have an absolute right to object to the use of your personal data for direct marketing. If you object to direct marketing, we will stop using your personal data for that purpose.

To exercise a right, email gdpr@actionfarm.co.uk, telephone 01743 762700, or write to us at Grange Court, Sitka Drive, Shrewsbury Business Park, Shropshire, SY2 6LG. We may need to confirm your identity before acting on a request. Rights are subject to conditions and exemptions in data protection law.

14. Complaints

Please contact us first if you have concerns about how we use personal data. You can email gdpr@actionfarm.co.uk, telephone 01743 762700, or write to Grange Court, Sitka Drive, Shrewsbury Business Park, Shropshire, SY2 6LG.

You also have the right to complain to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection:

Information Commissioner's Office	Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF Telephone: 0303 123 1113 ico.org.uk

15. Marketing

We may contact you about ACT products or services where this is permitted by law. We do not share personal data with third parties for their own unrelated marketing. You can ask us to stop direct marketing at any time by using the unsubscribe option in a message or contacting us using the details in section 1.

16. Changes and further information

We keep this privacy notice under review and will publish material changes at www.actionfarm.co.uk. The effective date and version number at the beginning of the notice show when it was last updated.

We aim to explain our processing clearly and in plain language. If anything in this notice is unclear, you require it in another format, or you would like further information, contact our Data Protection Officer using the details in section 1.