THE AUCTION COMPANY (UK) LTD

Data Protection (UK GDPR) Policy

Version 2.0 · Effective 23 November 2026

Document	Data Protection (UK GDPR) Policy
Version	2.0
Status	Approved by Ray Purchase, Managing Director.
Effective date	23 November 2026
Supersedes	GDPR Data Protection Policy dated July 2022
Policy owner	Ray Purchase, Managing Director (Data Protection Lead) – ray@theauctioncompany.co.uk
Review	At least annually, and whenever the law, ICO guidance or our processing changes

1. Introduction and scope

The Auction Company (UK) Ltd (**TAC**, **we**, **us**) is a property auctioneer and estate agent providing residential sales, commercial sales and auction services. We are registered in England and Wales (company number 12043088), with our registered office and trading address at 5 Regent Street, Rugby, Warwickshire, CV21 2PE. We are registered with the Information Commissioner's Office (ICO) under registration reference ZC310180. We are supervised by HMRC for anti-money laundering purposes (registration MLR-259742) and are a member of The Property Ombudsman.

TAC is the **data controller** for the personal data it processes about sellers, buyers, bidders, applicants, tenants and occupiers of properties we sell, referring agents, suppliers, website users and other contacts. This policy explains how we comply with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018 (DPA 2018)**, both as amended (including by the Data (Use and Access) Act 2025), and the Privacy and Electronic Communications Regulations 2003 (PECR) for marketing and cookies.

This policy applies to all directors, employees, agents, contractors and temporary staff of TAC, and to all personal data we hold in any format: paper files, computer systems, Outlook / Microsoft 365 email and files (including Microsoft Teams), our CRM (AUCTRA), our ID-check provider's system (Hipla), the online auction platform provided by EIG, call recordings made on our 3CX telephone system, and mobile phones or messaging apps (such as WhatsApp) used for TAC business. Failure to follow it may lead to disciplinary action.

Breaches of data protection law can result in ICO fines of up to **£17.5 million or 4% of total worldwide annual turnover**, whichever is higher, as well as claims for compensation and serious damage to our reputation.

2. Responsibility

Our **Data Protection Lead, Ray Purchase (Managing Director, ray@theauctioncompany.co.uk)**, is responsible for overseeing this policy, keeping our records of processing up to date, handling data subject requests and personal data breaches, and advising staff. The Managing Director has overall accountability, with the oversight of the board of directors. Every member of staff is responsible for handling personal data in line with this policy and must report any request, complaint or suspected breach to the Data Protection Lead immediately.

3. Key terms

- **Personal data:** any information relating to an identified or identifiable living individual, such as a name, email address, ID document, bank details, call recording or online identifier.
- **Special category data:** information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data (where used to identify someone), health, sex life or sexual orientation. **Criminal offence data** is treated in a similar way.
- **Processing:** anything done with personal data, including collecting, recording, storing, using, sharing, transferring and deleting it.

- **Data controller:** the organisation that decides why and how personal data is processed – TAC, for the data covered by this policy.
- **Data processor:** an organisation that processes personal data on TAC's behalf and on our instructions (for example, an IT or ID-check provider).
- **Personal data breach:** a security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. Data protection principles

We comply with the principles in Article 5 of the UK GDPR. Personal data must be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not used in a way that is incompatible with them;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept no longer than necessary; and
- kept secure, using appropriate technical and organisational measures.

We must also be able to demonstrate our compliance (**accountability**) – see section 17.

5. Personal data we process and our lawful bases

We only process personal data where we have a lawful basis under Article 6 of the UK GDPR. The main categories are:

Category	Examples	Main purposes	Lawful basis
Seller and buyer identity and contact details	Names, addresses, phone numbers, email addresses, correspondence	Taking instructions, marketing properties, running auctions and sales, progressing transactions	Contract; legitimate interests in running our business
AML / KYC records	Identity documents, proof of address, results of electronic ID checks, PEP and sanctions screening, beneficial ownership information, source-of-funds and source-of-wealth evidence	Customer due diligence and ongoing monitoring required by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017); preventing fraud	Legal obligation (MLR 2017). Criminal offence data revealed by checks: DPA 2018 Schedule 1 (see Appropriate Policy Document)
Bidding and registration records	Bidder registrations, proxy and telephone bidding forms, online auction platform accounts, bid history, deposits and holding fees, memoranda of sale	Running auctions, evidencing contracts, resolving disputes	Contract; legal obligation; legitimate interests (evidencing the sale)
Call recordings	Calls on our 3CX telephone system may be recorded, depending on the extension setting. The Managing Director's extension records incoming and outgoing calls, including telephone bids. Callers to the main line hear a recording message before they are connected. Recordings are stored in AUCTRA	Accurate record of instructions and bids, training and quality, preventing fraud, handling complaints and disputes	Legitimate interests (callers must be told calls may be recorded)
Financial and bank details	Bank account details, payment card transactions (processed by Opayo through the EIG platform), deposits, fees, refunds	Taking and returning payments and deposits, accounting and tax	Contract; legal obligation (accounting and tax law)

Category	Examples	Main purposes	Lawful basis
Marketing data	Contact details, property preferences, marketing preferences and consent records	Sending auction catalogues, property alerts and news	Consent for electronic marketing where PECR requires it; legitimate interests for existing customers (soft opt-in) and postal marketing, always with a right to opt out
Website and CRM data	Enquiry and offer forms, IP addresses, cookie and attribution data, CRM notes and activity history	Operating the website, responding to enquiries, managing customer relationships, improving our services	Legitimate interests; contract; consent where PECR requires it for cookies
Supplier, introducer and staff contacts	Names and business contact details of solicitors, TAC's agents, referring estate agents and other suppliers	Managing business relationships	Legitimate interests; contract

Special category and criminal offence data. We do not routinely seek special category data. We may hold it where a client tells us about health or accessibility needs or vulnerability (so that we can make reasonable adjustments), and AML screening may reveal information about criminal offences or political exposure. We will only process such data where a condition in Article 9 or 10 of the UK GDPR and Schedule 1 to the DPA 2018 applies (for example, explicit consent, or preventing or detecting unlawful acts and complying with regulatory requirements). Because we rely on Schedule 1 conditions (paragraphs 10 and 12) for criminal offence data arising from AML checks, we keep an **Appropriate Policy Document**, which explains how we comply with the data protection principles and our retention and erasure policies for that data.

Legitimate interests. Where we rely on legitimate interests we will consider, and record where appropriate, whether our interests are overridden by the individual's interests, rights and freedoms (a legitimate interests assessment).

6. Transparency and privacy notices

We tell people how we use their personal data through our **Privacy Notice**, published on our website and provided when we first collect data (for example, on instruction, bidder registration or website enquiry). Where we obtain personal data from someone else (such as an introducing agent or ID-check provider), we provide the privacy information within a reasonable period and at the latest within one month. Our privacy notice explains who we are, what data we collect, our purposes and lawful bases, who we share data with, international transfers, retention periods, individuals' rights and how to complain to us and to the ICO. Callers must be told that calls may be recorded – on incoming calls to the main line by a recorded message on our 3CX system before they are connected, and on recorded outgoing calls by the caller at the start of the call.

7. Purpose limitation, data minimisation and accuracy

We only collect the personal data we need for the purposes described in our privacy notice and do not use it for new, incompatible purposes without telling people and having a lawful basis. Staff must not collect excessive data, including copying ID documents beyond what MLR 2017 requires. We check data for accuracy when it is collected, update it when we are told of changes and correct or delete inaccurate data promptly.

8. Retention

We keep personal data only for as long as necessary for the purposes it was collected for, including to meet legal, accounting and regulatory requirements and to deal with complaints and legal claims. Our standard periods are:

Data	Retention period
Buyer and seller transaction records (instructions, contracts, bidding and sale records, correspondence), held in AUCTRA	6 years after the transaction completes or ends (the limitation period for contract claims)

Data	Retention period
AML / KYC records (customer due diligence documents and information, and records of transactions needed to reconstruct them)	5 years after the business relationship ends or the occasional transaction completes (held in AUCTRA and Hipla). After this, personal data obtained for AML purposes must be deleted unless we are required to keep it by law or for court proceedings, the person has consented, or we have reasonable grounds for believing it needs to be kept for legal proceedings (MLR 2017, regulation 40(5))
Financial and accounting records	6 years from the end of the financial year to which they relate
Personal data about suppliers and other service providers	Up to 5 years after the provider stops providing services to TAC
Call recordings (3CX, stored in AUCTRA)	2 years from the date of the call
Marketing data	Until the person unsubscribes or objects (we keep a suppression record so we do not contact them again). Marketing lists are reviewed at least annually and contacts no longer needed are removed
Website enquiries, CRM records for non-clients and cookie data	Only as long as needed to deal with the enquiry and any follow-up requested; reviewed at least annually and deleted when no longer needed. Cookies as stated in our Cookie Policy
Complaints records	6 years from the date the complaint is closed

Longer retention. Where the 6-year transaction period and the 5-year AML period differ, personal data obtained only for AML purposes is deleted at 5 years unless regulation 40(5) allows it to be kept. Any decision to keep it longer is recorded with the reason.

Preservation. Where personal data is the subject of a data subject request, a complaint, a dispute, a legal claim or a regulatory investigation, it must **not** be deleted, even if its normal retention period has passed, until the matter has been concluded. At the end of a retention period, data must be securely deleted or anonymised, and relevant processors told to do the same.

9. Data Protection Officer

TAC is not required to appoint a Data Protection Officer. Our core activities – selling property by auction and private treaty – do not involve regular and systematic monitoring of individuals on a large scale, or large-scale processing of special category or criminal offence data. Identity checks and AML screening are carried out because the law requires them for each client, not as large-scale monitoring. We will review this if our activities change. In the meantime our Data Protection Lead, Ray Purchase, carries out the day-to-day data protection role.

10. Security

We use appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing, loss, destruction or damage, including:

- access to customer systems (AUCTRA, Hipla and the TAC mailbox) limited to the Managing Director and TAC's agents, on a need-to-know basis, with strong, unique passwords;
- multi-factor authentication, which is used on our CRM (AUCTRA) and is being applied to all email (Microsoft 365) accounts;
- devices used for TAC business must be protected by a password or PIN and screen lock, kept up to date, and encrypted where the device supports it;
- business data on staff mobile phones and messaging apps (such as WhatsApp) kept to a minimum, protected and removed when no longer needed or when staff leave;
- secure storage and confidential shredding of paper records, including ID documents;
- care when sending personal data, especially bank details – checking recipients and verifying any change of bank details by phone using a known number;
- staff training, and regular review and testing of these safeguards.

11. Processors and other third parties

We share personal data only where necessary and lawful. Processors act on our instructions under a written contract that meets Article 28 of the UK GDPR. Other recipients are independent controllers and are responsible for their own compliance. Typical recipients are:

Recipient	Purpose	Role
EIG – online auction platform and property search (auctions.theauctioncompany.co.uk)	Property listings, bidder registration, online bidding, deposits and holding fees	Processor for TAC's auctions; EIG may also act as a controller for its own platform accounts
Opayo – card payments, through the EIG platform	Taking card payments, deposits and holding fees	Independent controller / processor for payment processing
Hipla (seller checks) and Landmark (buyer checks)	Electronic identity verification, PEP and sanctions screening; Hipla also stores AML records	Processors
AUCTRA – customer relationship management system	Client and transaction records, AML records, call recordings	Processor
Microsoft – Outlook and Microsoft 365	Email, files and Microsoft Teams	Processor
3CX – telephone system	Telephone calls and call recording	Processor
Our website hosting provider	Hosting www.theauctioncompany.co.uk and its enquiry forms	Processor
Apex Law (solicitors) and other parties' solicitors	Legal work, contracts and completing transactions	Independent controllers
TAC's agents and referring estate agents	Working with TAC on sales and purchases; receiving updates on referred clients	Agents working for TAC act under TAC's instructions; referring agents are independent controllers
Professional advisers, auditors and insurers	Advice, audit, insurance and claims	Independent controllers
HMRC, the National Crime Agency, the police, the ICO, The Property Ombudsman and other regulators	Legal and regulatory obligations, including suspicious activity reports	Independent controllers

Our current partners are EIG and Apex Law. Before using any new processor, we check that it gives sufficient guarantees and put an Article 28 contract in place. We will not sell personal data or share it with third parties for their own marketing without consent. Any disclosure required by law is documented and checked to make sure it is in fact required. We do not tell anyone (including the person concerned) about a suspicious activity report where this could amount to 'tipping off'.

12. International transfers

Some of our service providers may store or access personal data outside the UK. We will only transfer personal data outside the UK in line with Chapter V of the UK GDPR, namely where:

- the destination is covered by UK adequacy regulations (for example, the EEA, or US organisations certified under the UK Extension to the EU–US Data Privacy Framework); or
- appropriate safeguards are in place, such as the ICO's International Data Transfer Agreement (IDTA) or the International Data Transfer Addendum to the EU Standard Contractual Clauses, supported by a transfer risk assessment; or
- a specific exception applies, for example where the transfer is necessary for a contract with the individual.

TAC does not itself transfer personal data outside the UK. Some of our technology providers (for example, Microsoft) may store or access data outside the UK as part of their services. Before relying on a provider, we check its terms to confirm that any such transfer is covered by UK adequacy regulations or appropriate safeguards such as the IDTA or the UK Addendum, and we record this in our Record of Processing Activities.

13. Individuals' rights

Individuals have the following rights, subject to conditions and exemptions:

- to be informed about how their data is used (our privacy notice);
- of access to their personal data (a subject access request – see section 14);
- to have inaccurate data corrected and incomplete data completed;
- to have data erased in certain circumstances;
- to restrict processing in certain circumstances;
- to data portability, where processing is based on consent or contract and carried out by automated means;
- to object to processing based on legitimate interests, and an absolute right to object to direct marketing;
- rights relating to decisions with legal or similarly significant effects based solely on automated processing, including the right to human review. Results of electronic ID and AML checks must be reviewed by a person at TAC before any decision is made;
- to withdraw consent at any time where we rely on consent; and
- to complain to TAC and to the ICO (see section 16).

For all requests we will verify identity proportionately, respond without undue delay and within one calendar month (extendable by up to two further months for complex or numerous requests, telling the person within the first month), and act free of charge unless a request is manifestly unfounded or excessive. Erasure requests may be refused where we must keep the data, for example to comply with MLR 2017 or accounting law, or to establish, exercise or defend legal claims; we will explain why. Where we correct, erase or restrict data, we will tell the recipients we have shared it with, unless this is impossible or involves disproportionate effort.

14. Subject access request (SAR) procedure

A SAR can be made in any form – in writing, by email, by phone, in person or through social media – and does not need to mention data protection law. Any member of staff who receives one must pass it to the Data Protection Lead **on the same day**. The Data Protection Lead will:

1. **Log the request** in the SAR register, recording the date received, the requester, the data requested and the deadline.
2. **Verify identity** in a way that is proportionate to the request and the risk. We can rely on identification already held (for example, from AML checks) where it is adequate, and will not ask for more than is needed. If someone is acting for the requester (such as a solicitor), we will check their authority.
3. **Note the time limit.** We will respond within **one calendar month** of receipt. The time limit does not start until we have any identity verification we reasonably need, and may be paused while we wait for clarification that we reasonably need to identify the information requested. For complex or numerous requests we can extend the deadline by up to **two further months**, but we must tell the requester, with reasons, **within the first month**.
4. **Preserve the data.** From the moment a request is received, data that may fall within it must not be deleted or altered, even if its normal retention period expires.
5. **Search all relevant systems** reasonably and proportionately, including: email accounts (including former staff mailboxes); Microsoft Teams chats and files; the CRM (AUCTRA); the online auction platform (EIG); call recordings (3CX/AUCTRA); ID-check records (Hipla and Landmark); shared drives and document management; paper files; and staff mobile phones and messaging apps (including WhatsApp) used for TAC business.
6. **Review and redact third-party data.** Where information identifies another person, we will redact it, ask for their consent to disclose, or disclose it only where it is reasonable to do so without consent, taking account of any duty of confidence.
7. **Apply exemptions where relevant** under Schedule 2 to the DPA 2018, including legal professional privilege and the negotiations exemption (records of our intentions in negotiations with the requester,

where disclosure would prejudice those negotiations), and the crime and taxation exemption where disclosure would prejudice the prevention or detection of crime (including the restriction on tipping off). Exemptions are applied case by case and the reasons recorded.

8. **Respond free of charge.** We will provide a copy of the personal data in a commonly used format, together with the supplementary information required by Article 15 (purposes, categories of data, recipients, retention periods, the individual's rights, the source of the data and any international transfer safeguards). We may charge a reasonable fee or refuse only where a request is **manifestly unfounded or excessive**; if we refuse, we will explain why and tell the person they can complain to the ICO or seek a court remedy.
9. **Keep a record** of the response, including what was searched, what was disclosed, redactions and exemptions applied (with reasons), and the date sent. This record is kept for 6 years from the date of our response.

15. Personal data breaches

Any member of staff who discovers or suspects a breach (for example, an email sent to the wrong person, a lost phone or laptop, a phishing compromise or a payment-diversion attempt) must report it to the Data Protection Lead **immediately**. The Data Protection Lead will:

1. contain the breach and try to recover the data;
2. assess the risk to the individuals affected;
3. where the breach is likely to result in a risk to individuals' rights and freedoms, notify the **ICO without undue delay and, where feasible, within 72 hours** of becoming aware of it (giving reasons if notification is late);
4. where the breach is likely to result in a high risk, tell the affected individuals without undue delay, with advice on protecting themselves;
5. consider whether to inform the police, Action Fraud, banks or insurers; and
6. record every breach in the breach log, whether or not it is reported, with the facts, effects, decisions and remedial action.

Our processors must notify us of any breach affecting our data without undue delay after becoming aware of it (UK GDPR Article 33(2)).

16. Complaints

Anyone who is unhappy with how we have handled their personal data can complain to us at compliance@theauctioncompany.co.uk or by post to our Rugby address. We will acknowledge data protection complaints within 30 days, investigate them without undue delay and tell the person the outcome. They also have the right to complain to the **Information Commissioner's Office**: www.ico.org.uk, telephone 0303 123 1113.

17. Accountability, records and training

- We keep a **Record of Processing Activities** as required by Article 30 of the UK GDPR, and an **Appropriate Policy Document** for criminal offence data from AML checks. Both are internal documents, reviewed at least annually by the Data Protection Lead.
- We carry out a **data protection impact assessment** before any processing likely to result in a high risk (for example, new monitoring or call-recording technology, or new systems processing ID data).
- We build data protection into new systems and processes (**data protection by design and default**).
- Staff and agents must complete data protection training on joining and refresher training at least annually; the Data Protection Lead keeps training records.
- We keep registers of data subject requests, breaches and complaints, and review this policy at least annually.

18. Changes to this policy

We may update this policy from time to time to reflect changes in the law, ICO guidance or our business. This policy does not override the UK GDPR, the DPA 2018 or any other applicable law.

The Auction Company (UK) Ltd, registered in England and Wales, company number 12043088. Registered office: 5 Regent Street, Rugby, Warwickshire, England, CV21 2PE. ICO registration: ZC310180. Supervised by HMRC for anti-money laundering purposes, registration MLR-259742.