# GDPR DATA PROTECTION POLICY

## 1. Introduction

Under the General Data Protection Regulation (*(EU) 2016/679*) (the "**GDPR**"), everyone has rights relating to how their personal information is handled.

As Members of the Institute ('Members'), we act as data controllers (for the purposes of the GDPR) in relation to the personal information of individual buyers or sellers which we process in the course of operating a sale at an auction.

During the course of our activities, we will be required to collect, store and process personal information about individual buyers and/or sellers at an auction. We recognise the need to treat all such personal information in an appropriate and lawful manner.

## 2. About this Policy

The types of personal information that we may be required to handle include details of individuals': (i) names, addresses and contact details; (ii) financial details; (iii) how much livestock is bought or sold for; and (iv) bank details of buyers and sellers. Personal information, which may be held as part of a paper filing system or on a computer or other media, is subject to certain legal safeguards specified in the GDPR and other applicable data protection legislation. The GDPR imposes restrictions on how we may use personal information.

We recognise that the correct and lawful treatment of personal information will maintain confidence in the administration and effective running of the Institute, its' Members and any auction sale. Protecting the confidentiality and integrity of personal information is a critical responsibility which we take seriously at all times in the course of business. We acknowledge that the Institute and/or its' Members is exposed to potential fines of up to €20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

All of the Members are responsible for ensuring that they comply with the GDPR and this Policy is therefore necessary to implement appropriate practices, processes and controls and to demonstrate such compliance. Accordingly, we undertake to comply with this Policy at all times.

## 3. Definitions of Data Protection Terms

**"Data controller":** means the person or organisation that determines the purposes for which, and the manner in which, any personal data is processed. The data controller is responsible for establishing practices and policies in line with the GDPR. We are the data controller of all individual's personal data used by us in the course of administering the Institute.

**"Data processor":** means any person who processes personal data on behalf of a data controller. For example, we have appointed a central data processor who supplies software (including backing up data on the iCloud) to process personal information about Members on our behalf.

**"Data subject":** means a living, identified or identifiable individual about whom we hold personal data. All

data subjects have legal rights in relation to their personal data.

**"Personal data":** means any information relating to a living individual who can be identified from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

**"Personal data breach":** means any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of personal data is a personal data breach.

**"Processing or process":** means any activity that involves the use of personal data. It includes obtaining, recording, holding or storing the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

**"Sensitive personal data":** means information revealing an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and/or personal data relating to criminal offences and convictions. Sensitive personal data can only be processed under strict conditions.

## 4. Data Protection Principles

We adhere to the principles relating to the processing of personal data set out in the GDPR which require personal data to be:

- Processed lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency**).
- Collected only for specified, explicit and legitimate purposes (**Purpose Limitation**).
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (**Data Minimisation**).
- Accurate and where necessary kept up to date (**Accuracy**).
- Not kept in a form which permits identification of individuals for longer than is necessary for the purposes for which the data is processed (**Storage Limitation**).
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (**Security, Integrity and Confidentiality**).
- Not transferred to countries outside the European Economic Area (the "EEA") without appropriate safeguards being put in place (**Transfer Limitation**).
- Made available to data subjects in response to subject access requests and otherwise processed in accordance with the exercise of data subjects' rights (**Data Subject's Rights and Requests**).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (**Accountability**).

## 5. Fair and Lawful Processing

The GDPR is intended not to prevent the processing of personal information, but to ensure that it is done fairly and lawfully and without adversely affecting the rights of data subjects.

For personal data to be processed lawfully, certain conditions have to be met. Under the GDPR, these may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interests of the data controller or the third party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases, the data subject's explicit consent to the processing of sensitive personal data will be required.

Processing of Personal Data – Legitimate Interests

In the majority of cases, we will process personal information on the legal basis that such processing is necessary for (i) accounting practices and requirements; and (ii) the effective running of the auction. We will also process your information where it is necessary to do so in order for us to comply with any applicable laws or legislation.

As Members, we have a legal obligation to hold onto financial information for accountancy requirements and also have a clear legitimate interest in making sure that the any auction is administered correctly at all times. We must necessarily collect and process detailed personal information about individual buyers or sellers (please see examples above) in order for us to: (i) carry out our functions; and (ii) ensure the effective day-to-day operation of the auction. Processing of individual's personal information is therefore integral to the operation of an auction.

## 6. Transparency

Under the GDPR, personal data must be processed in a transparent manner. In particular, the GDPR requires data controllers to provide detailed, specific information to a data subject depending on whether the information was first collected directly from the data subject or from elsewhere. Such information must be provided through an appropriate privacy notice which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that the data subject can easily understand the information.

We shall ensure that a GDPR-compliant Privacy Notice is issued to individual buyers and sellers when personal data is first collected. The Privacy Notice issued must include all information required by the GDPR, including but not limited to the identity of the data controller, the lawful basis of processing, the purpose for which the personal data is to be processed, the categories of recipients to whom personal data may be disclosed, the criteria used to determine the retention period and details of the relevant data subject rights.

## 7. Purpose Limitation

Personal information must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner which is incompatible with those purposes.

We collect and process individual's personal information only for our legitimate purposes in administering and operating auctions and for accounting requirements. We are required to disclose our legitimate purposes for processing in our Privacy Notice issued to individuals.

We cannot use personal information for new, different or incompatible purposes from that disclosed to the individual when it was first obtained unless we have informed the individual of the new purposes and we have established a lawful basis for processing the personal information for the new purposes.

**8. Data Minimisation**

Under the GDPR, personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

As data controllers, we must not collect excessive personal data about individuals or any other third party. We must therefore ensure that all personal data which we collect and process is adequate and relevant for our intended purposes of administering and operating the effective running of an auction.

When personal data is no longer needed for specified purposes, it must be deleted or anonymised as appropriate.

**9. Accuracy**

As data controllers, we must ensure that the personal information we use and hold about individual buyers and sellers is accurate, complete, kept up to date and relevant to the purpose for which we collected it. We will therefore take steps to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We must take all reasonable steps to destroy or amend (as appropriate) inaccurate or out-of-date personal information.

**10. Storage Limitation – Retention of Personal Data**

Under the GDPR, personal information must not be retained for longer than is necessary for the purposes for which the data is processed.

Except as otherwise permitted or required by applicable law, we will only retain personal information for as long as necessary to fulfil the purposes we collected it for, as required to satisfy any legal, accounting, or reporting obligations, or as necessary to resolve disputes. To determine the appropriate retention period for personal information, we must consider the amount, nature, and sensitivity of the data, the potential risk of harm from unauthorised use or disclosure of the data, the purposes for processing the data, whether we can fulfil the purposes of processing by other means, and any applicable legal requirements.

We will typically retain personal information for the periods set out below, subject to any exceptional circumstances or to comply with laws or regulations that require a specific retention period:

- Information about individual buyers and sellers:

  Personal data about individual buyers and sellers will be retained by us for seven (7) years.

- Information about other service providers:

  Personal data will be retained for a period of up to five (5) years following the date that the relevant service provider ceases to provide services to the Members.

We will take all reasonable steps to destroy or erase from our systems all personal information that we no longer require in connection with the administration of any auction sale. This includes notifying third parties (e.g. service providers) of the need to destroy or erase such data where applicable.

**11. No requirement to appoint a Data Protection Officer**

Under the GDPR, a Data Protection Officer must be appointed where a data controller's core activities involve: (i) processing operations which require regular and systematic monitoring of data subjects on a large scale; or (ii) processing of sensitive personal data on a large scale.

As Members, it is clear that we do not carry out processing operations which involve regular and systematic monitoring of data subjects on a large scale. In addition, as we do not process individuals' or Members' sensitive personal data (e.g. health data), such processing does not constitute a core activity of the Institute or its Members and we do not process such data on a large scale. Accordingly, we are not required to appoint a Data Protection Officer.

**12. Data Security**

We will ensure that appropriate technical and organisational data security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss or destruction of, or damage to, personal data.

The GDPR requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction or erasure. In addition, we recognise that personal data may only be transferred to third party data processors (such as a central data processor who supplies any software and backs it up on the iCloud for the benefit of a Member) if they agree to comply with those procedures and policies, or if they put in place adequate data security measures.

We must maintain data security by protecting the confidentiality, integrity and availability of personal data, defined as follows:

- "Confidentiality" means that only people who have a need to know and are authorised to use the personal data can access it.
- "Integrity" means that personal data should be accurate and suitable for the purpose for which it is processed.
- "Availability" means that authorised users are able to access the personal data when they need it for authorised purposes.

Our data security procedures include, but are not limited to, the following:

- Segregation of personal data from other networks;
- Access controls, user authentications and passwords;
- Secure disposal of paper records and files;
- Training of individual Members on information security; and
- Written information security policies and procedures.

We will regularly evaluate and test the effectiveness of these safeguards to ensure the security of our processing of personal data.

Each Member is responsible for protecting the personal data which it holds and must therefore comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR to protect such data.

**13. Reporting a Personal Data Breach**

The GDPR imposes a duty on data controllers to notify a personal data breach to the Information Commissioner's Office ("ICO") within 72 hours after becoming aware of it, unless the relevant personal data breach is unlikely to result in a risk to the rights and freedoms of the relevant data subject. In addition, if a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the data controller must communicate the breach to the relevant data subject without undue delay. As data controllers, we will notify the ICO and/or any relevant data subject where we are legally required to do so.

We recognise that a personal data breach will be any data security incident that has affected the confidentiality, integrity or availability of personal data. There will be a personal data breach in the following circumstances: (i) whenever any personal data is lost, destroyed, corrupted or disclosed; (ii) if someone accesses the data or passes it on without proper authorisation; or (iii) if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Upon becoming aware of a personal data breach, we will contain the breach and shall assess the potential adverse consequences for the data subjects affected by the breach. Following such assessment, we will determine the risk to the rights and freedoms of the data subjects affected by the breach and shall take the following actions as appropriate:

- If we determine that the breach is likely to pose a risk to the data subjects affected (e.g. risk of identity theft or fraud, financial loss, damage to reputation, loss of confidentiality etc.), we will report the breach to the ICO within the 72 hour time period.
- If we determine that the breach is unlikely to result in a risk to the data subjects affected (e.g. because the relevant personal data is already publicly available and is not damaging or prejudicial to the relevant data subjects), we will not report the matter to the ICO.
- If we determine that the breach is likely to result in a high risk to the data subjects affected (e.g. the unauthorised disclosure of sensitive health information or the release of financial details or other personal data which will require the data subjects to take steps to protect themselves from the effects of the breach), we will immediately inform the data subjects of the breach, including details of the likely consequences of the breach and the measures proposed to be taken to deal with the breach.

We will maintain a written record of: (i) all personal data breaches which occur (including those which are not reported to the ICO); and (ii) all decisions made by us in relation to such breaches.

As data controllers, we must ensure that any data processors which act on our behalf are made subject to an obligation to notify us immediately on becoming aware of a personal data breach or, at the latest, no later than 48 hours after becoming aware of the breach. For each personal data breach, data processors will be required to provide us with: (i) a description of the personal data breach; (ii) an explanation of how the personal data breach occurred; (iii) the categories of personal data affected; (iv) the categories and

approximate number of data subjects concerned; (v) a description of the likely consequences of the personal data breach; (vi) a description of the measures it has taken to address the personal data breach; and (vii) a description of the proposed measures it intends to take to address the personal data breach, including, where appropriate, measures to mitigate the possible adverse effects of the personal data breach.

## 14. Data Subject's Rights And Requests

Under the GDPR, data subjects have certain rights in relation to their personal data. We will ensure that personal data held by us is processed in accordance with the exercise of data subjects' rights.

The GDPR provides data subjects with the following rights:

(i) The right to request access to any personal data held about them by the data controller. This is known as a subject access request ("SAR").

(ii) The right to object to or challenge processing which has been justified on the basis of the data controller's legitimate interests.

(iii) The right to ask the data controller to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed. This is known as the "right to be forgotten".

(iv) The right to ask the data controller to rectify inaccurate data or to complete incomplete data.

(v) The right to restrict processing of personal data in specific circumstances.

(vi) The right to object to decisions about them based solely on automated processing, including profiling.

(vii) The right to object to the data controller using the personal data held about them for direct marketing purposes.

(viii) In limited circumstances, the right to receive or ask for a copy of the personal data held about them to be transferred to a third party in a structured, commonly used and machine readable format. This is known as the right to "data portability".

(ix) The right to withdraw consent at any time to the processing of any data which has been processed by the data controller on the basis of consent.

(x) The right to receive certain information about the data controller's processing activities. This is achieved by providing the data subject with a Privacy Notice.

(xi) The right to prevent processing that is likely to cause damage or distress to the data subject or anyone else.

(xii) The right to request a copy of an agreement under which personal data is transferred outside of the EEA.

(xiii) The right to make a complaint to the ICO.

In the event that a member submits a request to the trustees to exercise any of the above rights, we shall take the following steps:

- Obtain sufficient information to verify the identity of the individual making the request. This is to avoid personal data about a Member or individual buyers or sellers being sent to a third party either inadvertently or as a result of deception.
- Assess the request promptly following receipt and in accordance with any timescales specified in the GDPR. In relation to the data subject rights at (i) to (viii) above, we must provide the individual with information on action taken in response to the request within 1 month of receipt of the request. However, if the request is complex or there are a number of requests, we may extend the period for issuing the final response by a further 2 months.
- Carry out appropriate searches on databases, systems, applications and other places where the relevant personal information which is subject to the request may be held. Identify the personal data which is subject to the request.
- Before responding to the request, we must consider whether there are any grounds under the GDPR to refuse the request, including any specific qualifications to the data subject rights or any general exemptions. For example, if the individual buyer or seller requests us to erase personal information held about them ("the right to be forgotten"), we may be able to refuse the request if: (i) the personal information is still necessary for the purposes for which it was collected; and (ii) we can also establish that we have overriding legitimate grounds to continue processing the information (e.g. if we require the information to enable us to respond to queries arising from accountancy practices). In addition, general exemptions may apply which would allow us to refuse requests in circumstances where it is necessary and proportionate to do so in order to safeguard various interests, including but not limited to: (i) the protection of the data subject or the rights and freedoms of third parties; or (ii) the enforcement of civil law claims.
- Following the completion of the assessment, we must issue a response to the individual's request within the relevant timescales under the GDPR (please see above).

Please see below for additional information on how we will respond to SARs and the right to be forgotten.

**15. Subject Access Requests ("SARs")**

When an individual submits a SAR for a copy of personal information held about them we shall take the following steps:

- Log the date on which the SAR was received (to ensure that the relevant timeframe of 1 month for responding to the SAR is met).
- Confirm the identity of the individual who has submitted the SAR. For example, we may request additional information from the individual to confirm their identity.
- Search databases, systems, applications and other places where the relevant personal information may be held.

- Confirm to the individual whether or not the relevant personal data is held by the relevant Member or the Institute.

Unless a relevant exemption applies (e.g. refusal of the SAR is necessary to safeguard the enforcement of civil law claims), we shall provide the individual with a copy of the personal information processed by us within 1 month of receipt of the SAR. If the request is complex, or there are a number of requests, we may extend the period for responding by a further 2 months. If we extend the period for responding we shall inform the individual within 1 month of receipt of the SAR and explain the reasons for the delay.

Before providing personal data to an individual in response to a SAR, we shall review the information being disclosed to ascertain whether the data includes personal data relating to other individuals. If it does, we may redact the personal data of those other individuals, unless those individuals have consented to disclosure of their personal data.

If the SAR is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing the personal data, or refuse to comply with the request.

If we are not going to respond to the SAR we shall inform the individual of the reasons for not taking action. We will also notify the individual of the option available to the individual to lodge a complaint with the ICO.

**16. Responding to Requests for the Erasure of Personal Data ("Right to be Forgotten")**

Under the GDPR, data subjects have the right, in certain circumstances, to request that we erase their personal data. We will be required to erase the personal data without undue delay if one of the following circumstances applies:

- The personal data is no longer necessary for the purposes for which it was collected or otherwise processed by the relevant Member;
- The data subject withdraws his or her consent to the processing of his or her personal data; and consent was the basis on which the information was obtained and there is no other legal basis for the processing;
- The data subject objects to the processing of his or her personal data on the basis of our entitlement to process without the need to obtain consent;
- The personal data has been unlawfully processed by the Member; or
- The personal data must be erased in order to comply with a legal obligation of the Member.

In most cases, we will not be required to comply with such a request if it is necessary for us to continue processing the relevant personal data for the purposes of administering the auction or for compliance with relevant accountancy requirements. In addition, there is also a specific exemption to the right to be forgotten in circumstances where continued processing of the relevant personal data is necessary for the establishment, exercise or defence of legal claims.

In the situation where an individual submits a request for erasure and it is clear that at least one of the above circumstances applies, we shall, unless there is a relevant exemption, take the steps set out below:

- Log the date on which the request was received (to ensure that the relevant timeframe of 1 month for responding to the request is met).
- Confirm the identity of the individual who has submitted the request; request additional information from the individual to do this.
- Search databases, systems, applications and other places where the relevant personal information may be held and erase such data within 1 month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further 2 months. If we extend the period for responding we shall inform the individual within 1 month of receipt of the request and explain the reasons for the delay.
- Communicate the erasure of the personal information to the relevant Member, the Institute and other relevant data processors and/or data controllers to whom the personal information has been disclosed, unless this is impossible or involves disproportionate effort.

If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of erasure, or refuse to act on the request.

If we are not going to respond to the request we shall inform the individual of the reasons for not taking action. We will also notify the individual of the option available to the individual to lodge a complaint with the ICO.

## 17. Accountability

As data controllers, we are responsible for implementing appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. Under the GDPR, we are now also required to demonstrate compliance with the data protection principles at all times.

We will therefore put in place adequate resources and controls in order to document compliance with the GDPR, including but not limited to:

- Integrating the new data protection requirements under the GDPR into all relevant internal and external documents, including but not limited to this Data Protection Policy, the Record of Processing Activities, the Privacy Notice issued to individuals and all contracts with any data processors.
- Training staff on the GDPR and relevant data protection matters.
- Testing the privacy measures implemented and conducting periodic reviews and audits to assess and demonstrate compliance.

## 18. Record Keeping

Under the GDPR, we are required to keep full and accurate records of all our data processing activities. This includes maintaining a record of: (i) all decisions in relation to the processing of personal data; (ii) all consents provided by individuals for the processing of their sensitive personal data (if applicable); (iii) all personal data breaches; and (iv) the exercise of data subjects' rights.

As data controllers, we are required to maintain a document known as a "Record of Processing Activities". As a minimum, this document must include the following: (i) name and contact details of the data controllers; (ii)

purposes of data processing; (iii) categories of data subjects; (iv) categories of persona data; (v) third party recipients of personal data; (vi) details of international data transfers (if applicable); (vii) retention periods for personal data; and (viii) a description of the data security measures in place.

**19. Training and Audit**

As Members, we must undergo adequate training to enable us to comply with our obligations as data controllers under the GDPR. This should include training on data subjects' rights, consent, legal basis for processing and responding to personal data breaches. We will maintain records of all such training.

We must also regularly test and audit our systems and processes to assess compliance with the GDPR. In particular, we must check to ensure that adequate controls and resources are put in place to ensure the proper use and protection of individual buyers and sellers' personal information.

**20. Data Sharing**

As Members, we will be required to share individual buyers or sellers' personal data with third parties on occasion. We will only share such data with third parties where it is necessary to do so. For example, we may be required to share individuals' personal data with the following third parties:

- Other Members;
- Professional advisers, including legal advisers and accountants;
- Insurers;
- Financial organisations and advisers;
- Suppliers and other service providers;
- Trade and business associates;
- The UK Government and other relevant public authorities and regulatory authorities;

Generally we will only share individuals' personal data with third party data processors and data controllers where certain safeguards and/or contractual arrangements have been put in place.

Where we share individuals' personal data with any third party data processor (such as an auditor or accountant), we must enter into a written contract with the data processor which includes the mandatory contractual provisions required under the GDPR.

Where we share individuals' personal data with third parties which use such information for their own purposes (i.e. other data controllers), we must enter into a contract with the other party which: (i) clearly describes the purposes for which the information may be used and any limitations or restrictions on the use of the information; and (ii) includes an undertaking from the other party that it shall at all times comply with the GDPR when processing the relevant personal data.

Where we are required by law to share individuals' personal data with any third party (e.g. the UK Government etc.), we shall put in place appropriate controls to ensure that the sharing of such data will be documented, regularly reviewed and verified to make sure that the data sharing is in fact required by law.

## 21. Changes to Data Protection Policy

We reserve the right to review and amend this Policy from time to time to ensure that it is consistent with the requirements of the GDPR and all other applicable data protection laws. We recognise that this Policy does not override the GDPR or any other applicable data protection laws or requirements.