DATA RETENTION POLICY

CONTENTS

1. PURPOSE

The purpose of this policy is to specify The Canterbury Auction Galleries (CAG) guidelines for retaining different types of personal data.

2. SCOPE

The scope of this policy covers all CAG personal data stored on company-owned, company-leased, and otherwise company-provided systems and media, regardless of location. These records may be created, received or maintained in hard copy or electronically.

3. POLICY STATEMENT

3.1. The need to retain personal data varies widely with the type of data. Some personal data can be immediately deleted and some must be retained until reasonable potential for future need no longer exists. This Data Retention Policy provides guidelines to ensure that all applicable regulations and CAG's rules on personal data retention are consistently applied throughout the organisation.

Reasons for data retention

3.2. Some personal data must be retained in order to protect the company's interests, comply with regulatory requirements, preserve evidence, and generally conform to good business practices. Personal data may be retained for one or several of the following reasons:

- Business requirements
- Regulatory requirements
- Possible litigation
- Accident investigation
- Security incident investigation
- Intellectual property preservation

Retention periods

3.3. Different types of data will be retained for different periods of time:

- Personal customer data: Personal data will be held for as long as the individual is a customer of the company plus 6 years.
- Personal employee data: General employee data will be held for the duration of employment and then for 6 years after the last day of contractual employment. Employee contracts will be held for 6 years after last day of contractual employment.
- Personal tax payments will be held for 6 years.
- Records of leave will be held for 6 years.
- Recruitment details: Interview notes of unsuccessful applicants will be held until after interview. This personal data will then be destroyed.
- Health and Safety: 6 years for records of major accidents and dangerous occurrences.
- Operational data: Most company data will fall in this category. Operational data will be retained for 6 years and renewed for continued clients.
- Critical data including Tax and VAT: Critical data must be retained for 6 years.

For more details, please refer to *Appendix 1 – Data Retention Schedule*

Retention of encrypted data

3.4. If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

Data duplication

3.5. When identifying and classifying CAG's personal data, it is important to also understand where that data may be stored, particularly for duplicate copies, so that this policy may be applied to all duplicates of the information.

Data destruction

3.6. When the retention timeframe expires, CAG will actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be approved only by a member or members of CAG 's senior management team.
The company specifically directs users not to destroy data in violation of this policy. Destroying data that a user may feel is harmful to himself or herself or destroying data in an attempt to cover up a violation of law or company policy is particularly forbidden.

4. RESPONSIBILITIES

Compliance, monitoring and review

4.1. The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing normal business activities at CAG rests with the Data Protection Officer.

4.2. All operating units' staff that deal with personal data are responsible for processing this data in full compliance with the relevant CAG policies and procedures.

Reporting in case of a data breach

4.3. In the case of possible data breach, the staff member(s) who first identifies the breach or incident, must immediately report all details of the incident to the Data Protection Officer.

4.4. The Data Protection Officer is required to report a personal data breach to the competent Data Protection Authority not later than 72 hours after becoming aware of it. The notification must include at least:
- a description of the nature of the breach, including, where possible, the categories and approximate number of data subjects and personal data records concerned;
- the name and contact details of the relevant Data Protection Officer or contact point;
- the likely consequences of the data breach; and
- measures taken or proposed by the controller to address the breach and/or mitigate its effects.

4.5. Where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the Data Protection Officer must communicate the breach to the data subject(s) without undue delay. The communication must describe in clear and plain language, the nature of the breach and at least:
- the name and contact details of the relevant Data Protection Officer or contact point;
- the likely consequences of the data breach; and
- measures taken or proposed by the controller to address the breach and/or mitigate its effects.

Records management

4.6. Staff must maintain all records relevant to administering this policy and procedure in electronic and paper form in a recognised CAG recordkeeping system.

4.7. All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

5. TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Data Backup: data copied to a second location, solely for the purpose of safe keeping of that data

Data Encryption: the process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored

Data Encryption Key: an alphanumeric series of characters that enables data to be encrypted and decrypted

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

6. RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Information Commissioners Office (ICO)
- The Canterbury Auction Galleries (CAG) Data Protection Policy

7. FEEDBACK AND SUGGESTIONS

7.1. CAG employees may provide feedback and suggestions about this document by speaking to their line manager.

8. APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	The Directors
Data Protection Officer	David Parker
Next Review Date	26/05/2024

Approval and Amendment History	Details
Original Approval Authority and Date	The Directors 26/05/2018
Amendment Authority and Date	

9. APPENDIX 1 – Data Retention Schedule

Please attach the Data Retention Schedule