Capital Karts Data Retention Policy

Introduction

In its everyday business operations Capital Karts collects and stores records of many types and in a variety of different formats. The relative importance and sensitivity of these records also varies and is subject to Capital Karts' security classification scheme.

It is important that these records are protected from loss, destruction, falsification, unauthorised access and unauthorised release and a range of controls are used to ensure this, including backups, access control and encryption.

Capital Karts also has a responsibility to ensure that it complies with all relevant legal, regulatory and contractual requirements in the collection, storage, retrieval and destruction of records. Of particular relevance is the European Union General Data Protection Regulation (GDPR) and its requirements concerning the storage and processing of personal data. Principle 5 of the Data Protection Act requires that data should not be kept longer than necessary for the purpose for which it is processed.

Therefore, in accordance with the Information Commissioner's Office published guidance, at Capital Karts, we are required to continuously:

- Review the data that we have;
- Review the length of time we keep personal data;
- Consider the purpose or purposes we hold the information, to assist us in deciding whether (and for how long) to retain it;
- Securely delete information that is no longer needed for this purpose or these purposes; and
- Update, archive or securely delete information once it goes out of date.

This control applies to all systems, people and processes that constitute Capital Karts' information systems, including all Board and Council members, employees, volunteers, suppliers and other third parties who have access to IoD systems.

The following documents are relevant to this policy:

- Privacy and Personal Data Protection Policy
- Personal Data Inventory
- Data Protection Impact Assessment Process
- Privacy Notice Procedure
- Personal Data Mapping Procedure

1 Records Retention and Protection Policy

This policy begins by establishing the main principles that must be adopted when considering record retention and protection. It then sets out the types of records held by Capital Karts and our general requirements before discussing record protection, destruction and management.

1.1 General Principles

There are a number of key general principles that must be adopted when considering record retention and protection policy. These are:

- Records must be held in compliance with all applicable legal, regulatory and contractual requirements
- Records must not be held for any longer than required
- The protection of records in terms of their confidentiality, integrity and availability must be in accordance with their security classification
- Records must remain retrievable in line with business requirements at all times
- Where appropriate, records containing personal data must be subject as soon as possible to techniques that prevent the identification of a living individual

1.2 Record Types and Guidelines

In order to assist with the definition of guidelines for record retention and protection, records held by Capital Karts are grouped into the categories listed in the table on the following page. For each of these categories, the required or recommended retention period and allowable storage media are also given, together with a reason for the recommendation or requirement.

Note that these are guidelines only and there may be specific circumstances where records need to be kept for a longer or shorter period of time. This should be decided on a case by case basis as part of the design of the information security elements of new or significantly changed processes and services.

Further information about records held by the organisation, including their security classifications and owners can be found in Capital Karts's Personal Data Inventory.

1.3 Retention of Data

Capital Karts will keep some forms of information for longer than others. Information should not be kept indefinitely, unless there are specific requirements. In line with principle 5 of the data protection act information should not be kept longer than is necessary.

Appendix 1, provides a breakdown of the timescales for the retention of various types of information. When data is no longer required it should be appropriately destroyed in line with the Confidential Waste Disposal policy, which outlines the procedure to be used for the disposal of information.

1.4 Use of Cryptography

Where appropriate to the classification of information and the storage medium, cryptographic techniques must be used to ensure the confidentiality and integrity of records.

Care must be taken to ensure that encryption keys used to encrypt records are securely stored for the life of the relevant records and comply with the organisation's policy on cryptography.

1.5 Media Selection

The choice of long term storage media must take into account the physical characteristics of the medium and the length of time it will be in use.

Where records are legally (or practically) required to be stored on paper, adequate precautions must be taken to ensure that environmental conditions remain suitable for the type of paper used. Back-up copies of such records should be taken by methods, such as scanning, where possible. Regular checks must be made to assess the rate of deterioration of the paper and action taken to preserve the records if required.

For records stored on electronic media such as tape, similar precautions must be taken to ensure the longevity of the materials, including correct storage and copying onto more robust media if necessary. The ability to read the contents of the particular tape (or other similar media) format must be maintained by the keeping of a device capable of processing it. If this is impractical an external third party may be employed to convert the media onto an alternative format.

1.6 Record Retrieval

There is little point in retaining records if they are not able to be accessed in line with business or legal requirements. The choice and maintenance of record storage facilities must ensure that records can be retrieved in a usable format within an acceptable period of time. An appropriate balance should be struck between the cost of storage and the speed of retrieval so that the most likely circumstances are adequately catered for.

1.7 Record Destruction

Once records have reached the end of their life according to the defined policy, they must be securely destroyed in a manner that ensures that they can no longer be used. The destruction procedure must allow for the correct recording of the details of disposal which should be retained as evidence.

1.8 Record Review

The retention and storage of records must be subject to a regular review process carried out under the guidance of management to ensure that:

- The policy on records retention and protection remains valid
- Records are being retained according to the policy
- Records are being securely disposed of when no longer required
- Legal, regulatory and contractual requirements are being fulfilled
- Processes for record retrieval are meeting business requirements

The results of these reviews must be recorded.

1.8.1 Annual review

This policy was approved by the Data Protection Officer on 24 May 2018. It will be reviewed annually by the Data Protection Team to ensure its relevance and alignment with best practice.