Capital Karts Data Breach Policy

1. Introduction

This policy is intended to be used when an incident has occurred that has resulted in, or is believed to have resulted in, a loss of personal data for which Capital Karts is a controller. This document should be used in conjunction with the Information Security Breach Procedure which describes the overall process of reacting to an incident affecting the information security of Capital Karts.

It is a requirement of the EU General Data Protection Regulation 2016 (GDPR) that incidents affecting personal data that are likely to result in a risk to the rights and freedoms of data subjects must be reported to the data protection supervisory authority without undue delay and where feasible, within 72 hours of becoming aware of it. In the event that the 72-hour target is not met, reasons for the delay must be provided.

Where an incident affects personal data, a decision must be taken regarding the extent, timing and content of communication with data subjects. The GDPR requires that communication must happen "without undue delay" if the breach is likely to result in "a high risk to the rights and freedoms of natural persons".

The actions set out in this document should be used only as guidance when responding to an incident. The exact nature of an incident and its impact cannot be predicted with any degree of certainty and so it is important that a good degree of common sense is used when deciding what to do. However, it is intended that the steps set out here will prove useful in ensuring that our obligations under the GDPR are fulfilled.

2. Definition/Types of Data Breach

For the purpose and context of this Policy, data security breaches include both confirmed and suspected incidents.

2.1 An incident is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to Capital Kart's information assets and/or reputation.

2.2 An incident may include, but is not restricted to, the following:

- Loss or theft of personal or sensitive data or equipment on which personal data is stored (e.g. loss of laptop, mobile phone, USB or paper records)
- Equipment theft or failure
- Unauthorised use of, access to or modification of personal data or information systems
- Attempts to gain unauthorised access to information or IT systems
- Unauthorised disclosure of personal/sensitive data
- Hacking
- Environmental circumstances (e.g. fire)
- Human error

3. Personal Data Breach Notification Procedure

Once it has been decided that a breach of personal data has occurred, there are two parties who may be required by the GDPR to be informed. These are:

1. The supervisory authority
2. The data subjects affected

It is not a foregone conclusion that the breach must be notified; this depends upon an assessment of the risk that the breach represents to *"the rights and freedoms of natural persons" (GDPR Article 33)*. The following sections describe how this decision must be taken and what to do if notification is required.

The Supervisory Authority

The supervisory authority for the purposes of the GDPR for Capital Karts is as follows:

Name:	Information Commissioners Office
Address:	Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Telephone:	01625 545 745
Fax:	01625 524 510
Email:	casework@ico.org.uk.

4. Deciding whether to notify the Supervisory Authority

The GDPR states that a personal data breach shall be notified to the supervisory authority *"unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons" (GDPR Article 33).* This requires that the organisation assess the level of risk before deciding whether or not to notify.

Factors to be taken into account as part of this risk assessment should include:

- Whether the personal data was encrypted
- If encrypted, the strength of the encryption used
- To what extent the data was pseudonymised (i.e. whether living individuals can reasonably be identified from the data)
- The data items included e.g. name, address, bank details, biometrics
- The volume of data involved
- The number of data subjects affected

- The nature of the breach e.g. theft, accidental destruction
- Any other factors that are deemed to be relevant

Parties involved in this risk assessment may include representatives from the following areas, depending on the nature and circumstances of the personal data breach:

- Senior management
- Business area(s)
- Technology
- Information security
- Legal
- Data protection officer
- Security team
- Others representatives as required

The risk assessment method, its reasoning and its conclusions should be fully documented and signed off by senior management. The result of the risk assessment should include one of the following conclusions:

1. The personal data breach does not require notification
2. The personal data breach requires notification to the supervisory authority only
3. The personal data breach requires notification both to the supervisory authority and to the affected data subjects

These conclusions may be subject to change based on feedback from the supervisory authority and further information that is discovered as part of the ongoing investigation of the breach.

5. How to notify the Supervisory Authority

In the event that it is decided to notify the supervisory authority, the GDPR requires that this be done *"without undue delay and, where feasible, not less than 72 hours after having become aware of it" (GDPR Article 33).* If there are legitimate reasons for not having given the notification within the required timescale, these reasons must be given as part of the notification.

The notification should be given via appropriate means to the Supervisory Authority, either by;

- using the form *GDPR-FORM-5 Personal Data Breach Notification Form* as a template;
- calling the ICO helpline on 0303 123 1113; or
- completing the form on the ICO website; https://ico.org.uk/media/for-organisations/documents/2258298/personal-data-breach-report-form-web-dpa-2018.doc

The following information must be given as part of the notification:

a) The nature of the personal data breach, including, where possible:

   i. Categories and approximate number of data subjects concerned

   ii. Categories and approximate number of personal data records concerned

b) Name and contact details of the data protection officer or other contact point where more information may be obtained

c) A description of the likely consequences of the personal data breach

d) A description of the measures taken or proposed to be taken to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects

e) If the notification falls outside of the 72-hour window, the reasons why it was not submitted earlier

Written confirmation should be obtained from the supervisory authority that the personal data breach notification has been received, including the date and time at which it was received. Where necessary, the GDPR allows the information to be provided in phases without undue further delay.

Documentation of the personal data breach, including its effects and the remedial action taken, will be produced as part of the Information Security Incident Response Procedure.

Data Subjects

6. Deciding whether to notify data subjects

The GDPR states that a personal data breach shall be notified to the data subject *"when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons" (GDPR Article 34).* Note the addition of the word "high" over and above the definition given in Article 33.

The risk assessment carried out earlier in this procedure (section 4) will have determined whether the risk to the rights and freedoms of the data subjects affected is judged to be sufficiently high to justify notification to them.

However, if measures have subsequently been taken to mitigate the high risk to the data subjects, so that it is no longer likely to happen, then communication to the data subjects is not required by the GDPR.

Notification to affected data subjects is also not mandated by the GDPR where it *"would involve disproportionate effort" (GDPR Article 34).* However, in this case a form of public communication should be used instead.

Again, this may change based on feedback from the supervisory authority and further information that is discovered as part of the ongoing investigation of the breach.

7. How to notify data subjects

Once it has been decided that the breach justifies communication to the data subjects affected, the GDPR requires that this be done without undue delay.

The communication to the affected data subjects *"shall describe in clear and plain language the nature of the personal data breach" (GDPR Article 34)* and must also cover:

a) Name and contact details of the data protection officer or other contact point where more information may be obtained

b) A description of the likely consequences of the personal data breach

c) A description of the measures taken or proposed to be taken to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects

In addition to the points required by the GDPR, it may be appropriate to offer advice to the data subject regarding actions they may be able to take to reduce the risks associated with the personal

data breach.

In most cases it will be appropriate to notify affected data subjects via letter or email or both in order to ensure that the message has been received and that they have an opportunity to take any action required.

8. Annual review

This policy was approved by Jamie Bedwell on 24 May 2018. It will be reviewed annually by Jamie Bedwell to ensure that the purpose still applies and every five years by the Board.