GDPR & Data Breach Policy

Contents

1. Background

In general, data security breaches are increasingly common occurrences whether caused through human error or via malicious intent. As the amount of data and information grows and technology develops, there are new ways by which data can be breached. Construction & Plant Assessments Ltd (CPA) have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly and protect personal data which it holds.

2. Aim

The aim of this policy is to standardise CPA's response to any data breach and ensure that they are appropriately logged and managed in accordance with the law and best practice, so that:

- Incidents are reported swiftly and can be properly investigated
- Incidents are dealt with in a timely manner and normal operations restored
- Incidents are recorded and documented
- The impact of the incident is understood, and action is taken to prevent further damage
- The ICO and data subjects are informed as required in more serious cases
- Incidents are reviewed, and lessons learned

3. Definition

Article 4 (12) of the General data protection Regulation ("GDPR") defines a data breach as:

"a breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

CPA is obliged under the GDPR to act in respect of such data breaches. This procedure sets out how the CPA will manage a report of a suspected data security breach.

The aim is to ensure that where data is misdirected, lost, hacked or stolen, inappropriately accessed or damaged, the incident is properly investigated, reported and any necessary action is taken to rectify the situation.

A data security breach can come in many forms, but the most common are as follows:

- Loss or theft of paper or other hard copy
- Data posted, e-mailed or faxed to the incorrect recipient

- Loss or theft of equipment on which data is stored
- Inappropriate sharing or dissemination-Staff accessing information to which they are not entitled
- Hacking, malware, data corruption
- Information is obtained by deception or “blagging”
- Equipment failure, fire or flood
- Unescorted visitors accessing data
- Non-secure disposal of data

In any situation where staff are uncertain whether an incident constitutes a breach of security, either report it to the Data Protection Officer (DPO) or the Senior Information Risk Owner (SIRO)(Director). If there are IT issues, such as the security of the network being compromised, IT should be informed immediately in addition to the SIRO.

4. Scope

CPA’s policy applies to all staff, management, visitors, contractors, partner organisations and data processors acting on behalf of CPA regardless of format.
It is to be read in conjunction with CPA’s Policy privacy statement.

5. Responsibilities

Information Users

The GDPR applies to both Data Controllers, Processors and to Data Handlers. Therefore, all information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

Directors

Are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.

Responsible Officers

Lead responsible officers (DPO, SIRO) will be responsible for overseeing management of the breach in accordance with the Data Breach Reporting Plan. Suitable further delegation may be appropriate in some circumstances.

6. Reporting a Breach

Internal

Suspected data security breaches should be reported promptly to the DPO as the primary point of contact on 01709 868181, email: info@cpassessments.co.uk
The report must contain full and accurate details of the incident including who is reporting the incident, and what classification of data is involved.
The incident report form should be completed as part of the reporting process. See Data Breach Reporting Template.
Once a data breach has been reported an initial assessment will be made to establish the severity of the breach.

All data security breaches will be centrally logged by the DPO/SIRO to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes.

External
Article 33 of the GDPR requires CPA as data controller to notify the ICO only when the breach "is likely to result in a risk to the freedoms and rights of natural persons". Such a breach also must be communicated to the data subject (with certain exceptions). Notification must be made "without undue delay" and within 72 hours of becoming aware of it. If CPA fails to do this, it must fully explain the reason for the delay.

Article 33(5) requires that CPA must maintain documentation on data breaches, their nature and remedial action taken.

A report to the ICO must contain information as to the nature of the breach, categories of data, number of data records, number of people affected, name and contact details of DPO, likely consequences of the breach and action taken.

7. Data Breach Management Plan
CPA's response to any reported data security breach will involve the following four elements.

- Containment and Recovery
- Assessment of Risks
- Consideration of Further Notification
- Evaluation and Response

Each of these four elements will need to be conducted in accordance with the checklist.
An activity log recording the timeline of the incident management should also be reflected in this document.

NB. This reflects current guidance from the ICO, which may be likely to change.

8. Disciplinary
Staff, management, visitors, contractors, partner organisations and data processors acting on behalf of CPA who act in breach of this policy may be subject to disciplinary procedures or other appropriate sanctions.

9. Review
This document shall be subject to annual review by the DPO/SIRO.

10 References

- **The GDPR**

https://gdpr-info.eu

- **ICO GUIDANCE ON DATA BREACHES**

https://ico.org.uk/for-organisations/report-a-breach/

http://www.privacy-regulation.eu/en/article-33-notification-of-a-personal-data-breach-to-the-supervisory-authority-GDPR.htm

Data Breach Reporting Template

	Report by:	Name: Title: Date:
1	Summary of event and circumstances	Who, what, when, who etc.
2	Type and amount of personal data	Title of document(s)-what information is included-name, contact details, financial, sensitive or special category data.
3	Action taken by recipient	
4	Action taken to retrieve data and respond to breach	
5	Procedure/policy in place to minimise risk	Communication, secure storage, sharing, exchange.
6	Breach of policy/procedure by officer/member	Has there been a breach of policy and has appropriate management action been taken?
7	Details of notification to data subject. Complaint received?	Has data subject been notified? If not, explain why. What advice has been offered?
8	Details of Data Protection training provided.	Date of most recent training by staff/ organisation involved
9	Risk assessment and changes need to prevent further data loss	
10	Conclusions and learning points	