Commonwealth Games England

Data Breach Incident Management Policy

Introduction

Commonwealth Games England (CGE) processes a range of personal data in the normal course of its business. Whilst every effort has been made to ensure that the business systems and processes are robust and secure from design to operation, risks can be reduced but not eliminated. In order to reduce the potential adverse consequences of the residual risk CGE maintains a comprehensive Incident Management policy.

Policy scope

This policy applies to:

- The head office of CGE, and any permanent or temporary satellite offices including home working.
- All employees of CGE, including volunteers and secondees
- All contractors, suppliers and any other people working on behalf of CGE including Team Leaders

It applies to any Data Breach event involving any of the personal data that the company holds relating to individuals.

Why this policy exists

This Incident Management policy ensures that CGE

- Communicates to its employees what constitutes a data breach, how to recognise one and how to react (including escalation routines).
- Has a robust incident management framework, with clearly allocated roles and responsibilities.
- Can react in the timeframes required by the suite of Data Protection legislation in force in the UK.

Responsibilities

Everyone who works for or with CGE has some responsibility for ensuring that any data breach is highlighted and managed in an effective and timely manner.

However, these people have key areas of responsibility:

- The Board of Directors, supported by its operating committees, is ultimately responsible for ensuring that CGE meets its legal obligations and ensures that adequate resource is made available for the implementation of this policy.
- The Chief Executive is responsible for:
    - Reviewing, updating and amending this policy as required as the business and legislative framework develop over time. As a minimum requirement this policy will be reviewed and re-approved by the Board at least annually.
    - Implementing organisational (including external expertise as required) and technology controls to support the functioning of this policy, and for ensuring that all users receive adequate training to understand and execute this policy.

- Keeping the Board updated about data protection responsibilities, risks and issues.

- The Chief Financial Officer is responsible for:
  - The day to day maintenance and updating of this policy.
  - Ensuring that this Incident Management Policy is tested at least once per year.
  - Leading the execution of this policy in the event of an incident occurring.
  - Ensuring that another member of the management team is suitably trained to act as a deputy in the event of the Chief Financial Officer being unavailable.
- All other employees and other non-employed personnel are responsible for
  - Ensuring that they understand how to recognise and report a suspected Data Breach Incident in line with this policy.
  - Reporting any suspicions or concerns about the day-to-day operations of the business which may lead to a Data Breach Incident

What is a Data Breach?

A personal data breach means a breach of operational protocols or data security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data or being "hacked" in the conventional sense.

As a result, the most likely potential sources of a Data Breach Incident for CGE are

1. An incident which occurs at one of CGE's 3rd party data processors who carry out primary data processing activities.
2. An incident involving the CGE data server
3. An incident involving a hard copy file
4. An incident originating with an employee or person working on behalf of CGE. These are likely to be
   - Incorrectly addressed e mails sent outside of CGE.
   - Data sent outside of CGE without appropriate consent or another legal basis under UK GDPR.
   - Accidental data editing / erasure in the course of day-to-day operations.
   - Loss of a piece of hardware such as a laptop or mobile phone with a company account loaded (by accident or theft).
   - Loss of sign on credentials for one of more of CGE's business systems

Initial Reporting of a Data Breach Incident

In the event of a data breach occurring at one of CGE's third-party data processors they are required by their contract to notify CGE immediately with details of the nature, scope and timing of the incident. The notification will normally be directly to the Chief Financial Officer, but in the unlikely event that another employee receives the notification then that employee will notify the Chief Financial Officer immediately.

In the event of a data breach originating with, or being discovered by, an employee (or volunteer, secondee, team leader or contractor) of CGE the individual should immediately notify the Chief Financial Officer (or nominated deputy in the absence of the Chief Financial Officer) who will follow through as prescribed in this policy. All employees are instructed to

operate on the basis of “if in doubt, report it” so that any grey areas of interpretation or understanding result in a failsafe condition.

Responding to a Data Breach Incident Report

Step 1 – identify, contain and minimise impact

The Chief Financial Officer, supported by the management team (including external resources if required) and, where relevant, the third-party data processors’ support staff will immediately commence an investigation process to determine

- The nature and scope of the incident, including
    - What systems / hardware / credentials are affected?
    - What type of data is affected / at risk?
    - How many records are affected / at risk?
    - What is the residual situation after the implementation of rectification processes?
- Is the incident contained and unable to spread further or get worse?
    - If “yes”, continue the investigation
    - If “no”, take actions to contain the incident
        - For a third-party processor or the on-site server take the system off line immediately
        - In the case of lost or stolen hardware use available management tools to shut down / disable / wipe down the hardware
        - In the case of lost or stolen credentials disable the account(s) immediately
        - For misdirected e mails take steps to recall or delete the messages, including communicating with the unplanned recipients. Request confirmation from the unplanned recipient that the e mail has been deleted immediately.

The Chief Financial Officer will ensure that a thorough log and day book of the process and its inputs / outputs is maintained.

Step 2 – assessment, reaction and reporting

Having worked through step 1, the Chief Financial Officer, supported by the management team (including external resources if required) and, where relevant, the third-party data processors’ support staff will immediately begin a process to assess the impact of the incident and decide on what, if any, external communications are required (to the ICO, to the data subject(s), to a 3rd party processor).

All external communications will be managed and channeled by the Chief Financial Officer.

Guidance on the process, its outcomes and required timescales is available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/ .

The Chief Financial Officer will ensure that a thorough action log and day book of the process and its inputs / outputs is maintained.

If there is any evidence or suspicion that any criminal activity has taken place the Chief Financial Officer will ensure that a separate legal report is prepared, and the relevant police authorities are informed as soon as possible.

Step 3a – remedial action to return the system(s) to use

This stage is ideally carried out in parallel with step 2 and focusses on business continuity.

Based on the outputs from step 1, the Chief Financial Officer, supported by the management team (including external resources if required) and, where relevant, the third-party data processors' support staff will

- Re-confirm that the initial incident is fully contained.
- Identify what rectification steps can be implemented
    - Immediately
    - With additional work
- Prepare a prioritised plan to return the affected systems to full use. If necessary, this return to use plan should include controlled re-introduction of user groups on a department-by-department basis.
- Communicate the plan to the relevant management team members, including board and A&F committee members as appropriate.
- Execute the return to use plan

The Chief Financial Officer will ensure that a thorough action log and day book of the process and its inputs / outputs is maintained.

Step 3b – remedial action to recover lost data

This stage is ideally carried out in parallel with step 2 and focusses on data reclamation.

Based on the outputs from step 1, the Chief Financial Officer, supported by the management team (including external resources if required) and, where relevant, the third-party data processors' support staff will

- Re-confirm that the initial incident is fully contained.
- In the case of accidental data loss take steps to recover the lost data and / or ensure that it is permanently deleted by the unintended recipients.
- If data has been accidentally deleted take steps to restore the relevant back up data.

The Chief Financial Officer will ensure that a thorough action log and day book of the process and its inputs / outputs is maintained.

Step 4 – learning and corrective action

Once steps 1, 2 and 3 are completed the Chief Financial Officer, supported by the management team (including external resources if required), will review the incident, the incident management process and the eventual outcomes. The review process will generate a report for the board of Directors which

- Details the incident, its discovery and the timeline of action / reaction.
- Details the outcomes of the incident.
- Details the effectiveness of the remedial actions taken.
- Applies the benefit of hindsight to identify any weaknesses or areas for improvement in the way the incident was managed.
- Identifies any remedial action required
    - With third party suppliers.
    - With CGE operating systems and disciplines.
    - With employees or other personnel working for CGE (additional training, disciplinary sanction etc.).
    - In terms of changing the provisions of this Data Breach Incident Management Policy based on its effectiveness in dealing with the incident.

The report and any CGE board feedback will be held on file for future reference and will be used as part of the annual review of this policy.